Logical Operations℠

choice

CompTIA® A+® Certification: Exam 220-801

Part Number: 093002
Course Edition: 2.2

Acknowledgements

PROJECT TEAM

Content Developer	*Media Designer*	*Content Editor*
Gail Sandler Kelly Popen Pamela J. Taylor	Alex Tong	Tricia Murphy Angie French

Notices

DISCLAIMER

While Logical Operations, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The name used in the data files for this course is that of a fictitious company. Any resemblance to current or future companies is purely coincidental. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Logical Operations is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. Use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by, nor any affiliation of such entity with Logical Operations. This courseware may contain links to sites on the internet that are owned and operated by third parties (the "External Sites"). Logical Operations is not responsible for the availability of, or the content located on or through, any External Site. Please contact Logical Operations if you have any concerns regarding such links or External Sites.

TRADEMARK NOTICES

Logical Operations and the Logical Operations logo are trademarks of Logical Operations, Inc. and its affiliates.

CompTIA® A+® is a registered trademark of CompTIA, Inc. in the U.S. and other countries. The other CompTIA products and services discussed or described may be trademarks or registered trademarks of CompTIA, Inc.

Microsoft® Windows® is a registered trademark of Microsoft Corporation in the U.S. and other countries. The other Microsoft products and services discussed or described may be trademarks or registered trademarks of Microsoft Corporation. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright © 2013 Logical Operations, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without express written permission of Logical Operations, 3535 Winton Place, Rochester, NY 14623, 1-800-456-4677 in the United States and Canada, 1-585-350-7000 in all other countries. Logical Operations' World Wide Web site is located at **www.logicaloperations.com.**

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. Do not make illegal copies of books or software. If you believe that this book, related materials, or any other Logical Operations materials are being reproduced or transmitted without permission, please call 1-800-456-4677 in the United States and Canada, 1-585-350-7000 in all other countries.

About This Course

If you are getting ready for a career as an entry-level information technology (IT) professional or personal computer (PC) service technician, the CompTIA® A+® Certification (Exam 220-801) course is the first step in your preparation. The course will build on your existing user-level knowledge and experience with personal computer software and hardware to present fundamental skills and concepts that you will use on the job. In this course, you will acquire the essential skills and information you will need to install, upgrade, repair, configure, troubleshoot, optimize, and perform preventative maintenance of basic personal computer hardware and operating systems.

The CompTIA A+ Certification (Exam 220-801) course can benefit you in two ways. Whether you work or plan to work in a mobile or corporate environment where you have a high level of face-to-face customer interaction, where client communication and client training are important, or in an environment with limited customer interaction and an emphasis on hardware activities, this course provides the background knowledge and skills you will require to be a successful A+ technician. It can also assist you if you are preparing to take the CompTIA A+ certification examination, 2012 objectives (exam number 220-801), one of the exams required in order to become a CompTIA A+ Certified Professional. The other exam required in order to become a CompTIA A+ Certified Professional is exam number 200-802; the material to assist you in preparing for that exam is covered in the CompTIA A+ Certification (Exam 220-802) course.

Course Description

Target Student

This course is intended for anyone with basic computer user skills who is interested in obtaining a job as an IT professional or PC technician. In addition, this course will help prepare students to achieve a CompTIA A+ Certification.

Course Prerequisites

Students taking this course should have the following skills: end-user skills with Windows®-based personal computers, including the ability to: browse and search for information on the Internet; start up, shut down, and log on to a computer and network; run programs; and move, copy, delete, and rename files in Windows Explorer. Students should also have basic knowledge of computing concepts, including the difference between hardware and software; the functions of software components, such as the operating system, applications, and file systems; and the function of a computer network.

An introductory course in a Windows operating system, or equivalent skills and knowledge, is required. Students can take any one of the following Logical Operations courses: *Introduction to Personal Computers: Using Windows® XP* or I*ntroduction to Personal Computers: Using Windows® 7*.

The following Logical Operations courses are also recommended: *Windows® XP: Introduction* or *Microsoft® Windows® 7: Level 1*.

Course Objectives

In this course, you will install, upgrade, repair, configure, optimize, troubleshoot, and perform preventative maintenance on basic personal computer hardware and operating systems.

You will:

- Identify the hardware components of a computer.
- Identify the operational procedures that should be followed by PC technicians.
- Identify and configure peripheral components.
- Manage system components.
- Identify the hardware and software requirements for custom client environments.
- Identify network technologies used to configure and maintain SOHO networks.
- Support laptops.
- Support printers.
- Implement concepts and techniques used to secure computing devices and environments.

The LogicalCHOICE Home Screen

The LogicalCHOICE Home screen is your entry point to the LogicalCHOICE learning experience, of which this course manual is only one part. Visit the LogicalCHOICE Course screen both during and after class to make use of the world of support and instructional resources that make up the LogicalCHOICE experience.

Log-on and access information for your LogicalCHOICE environment will be provided with your class experience. On the LogicalCHOICE Home screen, you can access the LogicalCHOICE Course screens for your specific courses.

Each LogicalCHOICE Course screen will give you access to the following resources:

- eBook: an interactive electronic version of the printed book for your course.
- LearnTOs: brief animated components that enhance and extend the classroom learning experience.

Depending on the nature of your course and the choices of your learning provider, the LogicalCHOICE Course screen may also include access to elements such as:

- The interactive eBook.
- Social media resources that enable you to collaborate with others in the learning community using professional communications sites such as LinkedIn or microblogging tools such as Twitter.
- Checklists with useful post-class reference information.
- Any course files you will download.

- The course assessment.
- Notices from the LogicalCHOICE administrator.
- Virtual labs, for remote access to the technical environment for your course.
- Your personal whiteboard for sketches and notes.
- Newsletters and other communications from your learning provider.
- Mentoring services.
- A link to the website of your training provider.
- The LogicalCHOICE store.

Visit your LogicalCHOICE Home screen often to connect, communicate, and extend your learning experience!

How to Use This Book

As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of activities designed to enable you to practice the guidelines and procedures as well as to solidify your understanding of the informational material presented in the course. Procedures and guidelines are presented in a concise fashion along with activities and discussions. Information is provided for reference and reflection in such a way as to facilitate understanding and practice.

Data files for various activities as well as other supporting files for the course are available by download from the LogicalCHOICE Course screen. In addition to sample data for the course exercises, the course files may contain media components to enhance your learning and additional reference materials for use both during and after the course.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the course. You will also find an index to assist in locating information within the instructional components of the book.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking

advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Course Icons

Watch throughout the material for these visual cues:

Icon	*Description*
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** helps make you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.
	LearnTO notes show you where an associated LearnTO is particularly relevant to the content. Access LearnTOs from your LogicalCHOICE Course screen.
	Checklists provide job aids you can use after class as a reference to performing skills back on the job. Access checklists from your LogicalCHOICE Course screen.
	Social notes remind you to check your LogicalCHOICE Course screen for opportunities to interact with the LogicalCHOICE community using social media.
	Notes Pages are intentionally left blank for you to write on.

Lesson 1: Hardware Fundamentals

Lesson Time: 2 hours, 10 minutes

A very large percentage of the work that most IT technicians do entails working with hardware, including installing, upgrading, repairing, configuring, maintaining, optimizing, and troubleshooting computer components. To install and configure computer hardware, you need to recognize the basic components that constitute most personal computers, along with the functionality that each component provides to the computing experience. In this lesson, you will identify hardware components and how they function.

Preparing for a career in computer support and maintenance can be a daunting task. A good place to start is with the basics: the essential hardware components that you find in most computers. Identifying hardware components and their roles give you a solid base on which to build the knowledge and skills you need to install, configure, and troubleshoot computer hardware.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Topic A:
  - Objective 1.1
- Topic B:
  - Objectives 1.5, 1.7, 1.12
- Topic C:
  - Objectives 1.7, 1.11

Topic A: Computer System Components

In this lesson, you will identify the hardware components of a computer. The first step is to identify the hardware that you will find in virtually all computer systems. In this topic, you will identify computer system components.

If you are not familiar with the various components that a computer is made up of, it can seem like a jigsaw puzzle. Like most puzzles, each part of a computer connects to other parts in a specific place, but generally, you will find that the pieces fit together almost exactly the same way from one system to another. To help you put the puzzle together, you need to understand what these pieces look like and what they do.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.1: Configure and apply BIOS settings.

Common Computer Components

Computing components are the physical devices that are required for a computer to operate properly. There are four main categories of components in a typical computer.

Component	*Description*
The *system unit*	The system unit, also commonly referred to as the CPU, or the tower, is the main component of a computer, which houses most of the other devices that are necessary for the computer to function. Traditionally, it is comprised of a chassis and internal components, such as the system board, the microprocessor, memory modules, disk drives, adapter cards, the power supply, fans and other cooling systems, and ports for connecting external components such as monitors, keyboards, mice, and other devices. System units are also often referred to as boxes, main units, or base units. In some newer computer models, the system unit is incorporated with the display screen and referred to as an all-in-one computer. Similar to laptops, the system unit is integrated into a smaller configuration, which may make it harder to manage or replace the system unit components.
	A display device is a personal computer component that enables users to view the text and graphical data output from a computer. Display devices commonly connect to the system unit via a cable, and they have controls to adjust the settings for the device. They vary in size and shape, as well as the technologies used. Common terms for various types of display devices include display, monitor, screen, cathode ray tube (CRT), *liquid crystal display (LCD),* and flat-panel monitors.

Display devices	
Input devices	An input device is a personal computer component that enables users to enter data or instructions into a computer. Common input devices include keyboards and computer mice. An input device can connect to the system unit via a cable or a wireless connection.
External devices	You can enhance the functionality of practically any personal computer by connecting different types of external devices to the system unit. Also called peripheral devices, external devices can provide alternative input or output methods or additional data storage. You connect external devices to the system unit via cable or a wireless connection. Some devices have their own power source, while others draw power from the system. Common examples of external devices include microphones, cameras, scanners, printers, and external drives.

Computer Cases

The *computer case* is the enclosure that holds all of the components of your computer. Computer

cases come in several sizes and arrangements. Some are designed to hold many internal components and have a lot of room to work around those components. These are usually tower or desktop cases and take up a good deal of room. Other cases are designed to use a minimum amount of space. The trade-off is that the interior of the case is often cramped, with little room for adding additional components. Because the tower proved to be popular, there are now several versions of the tower model. These include:

- Full tower, which is usually used for servers or when you will be installing many drives and other components.
- Mid tower, which is a slightly smaller version of the full-size tower.
- Micro, or mini tower, which is the size that replaces the original desktop case in most modern systems.
- Slim line, which is a tower case that can be turned on its side to save room

The Motherboard

The *motherboard* is the personal computer component that acts as the backbone for the entire computer system. Sometimes called the *system board*, it consists of a large, flat circuit board with chips and other electrical components on it, with various connectors. Some components are *soldered* directly to the board, and some components connect to the board by using slots or sockets.

Figure: A motherboard.

The CPU

The *central processing unit (CPU)* is a computer chip where most of the computing calculations take place. On most computers, the CPU is housed in a single microprocessor module that is installed on the system board in a slot or a socket.

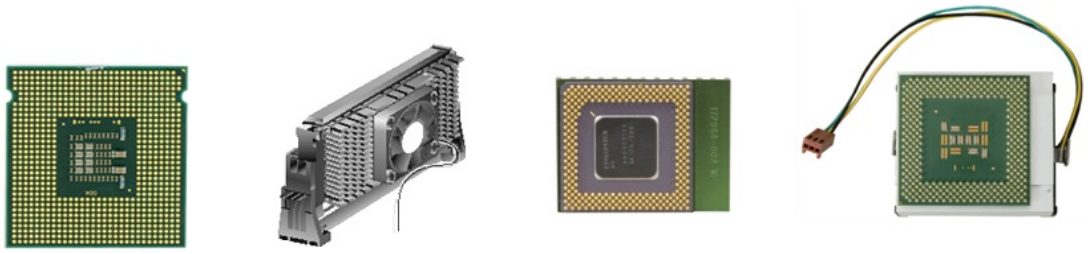


Figure: CPUs.

Multicore Processors

Since mid-to-late 2000, the trend has been to build processors with two or more individual CPUs that work in parallel and that are contained in a single chip. Two or more individual processors can share a workload more efficiently than a single processor. Dual-core and quad-core processors are engineered to include two to four cores on a single chip, while hexa- and octa-core processors include six and eight cores, respectively.

Multi-CPU Motherboards

Prior to the development of multicore processors, some hardware manufacturers offered additional processing power by designing motherboards that could hold more than one CPU. With the advent of the multicore processors, these are less common in personal computers, but they are still widely used in server machines.

Memory

Memory is the computer system component that provides a temporary workspace for the processor. Memory refers to modules of computer chips that store data in a digital electronic format, which is faster to read from and write to than tape or hard drives. Memory chips each contain millions of transistors etched on one sliver of a semiconductor. *Transistors* are nothing more than switches that can be opened or closed. When a transistor is closed, it conducts electricity, representing the binary number 1. When it is opened, it does not, representing the binary number 0.

There are two types of memory used in computer systems: *Random Access Memory (RAM)* and *Read-Only Memory (ROM)*. RAM is a computer storage method that functions as a computer's main memory. This type requires a constant power source to access the data stored within the RAM. However, data stored on ROM is saved and stored without a constant power source. Once data is written to ROM, it cannot be modified easily.

Volatile and Non-volatile Memory

Memory is considered to be either volatile or non-volatile:

- Volatile memory stores data temporarily and requires a constant source of electricity to keep track of the data stored in it. When the power is no longer available, the data stored in volatile memory is lost. The computer's main RAM is an example of volatile memory. The computer can both read the data stored in RAM and write different data into the same RAM. Any byte of data can be accessed without disturbing other data, so the computer has random access to the data in RAM.

- Non-volatile memory retains the information stored on it whether or not electrical current is available. ROM is an example of non-volatile memory.

Figure: A sample memory module.

The System Bus

In computer communications, a *bus* is a group of wires or electronic pathways that connect components. The *system bus* is the wires, or *traces,* on the motherboard that provide the main communication path between the CPU and memory. The system bus enables data transfer between the CPU, memory, and the other buses in the computer, which connect other system components such as hard drives and adapter cards. It is sometimes referred to as the frontside bus or local bus.

Storage Devices

A *storage device* is a computer system component, such as a hard drive, that enables users to save data for reuse at a later time, even after the personal computer is shut down and restarted. Storage devices can save data magnetically, optically, or electronically, depending on their design.

Figure: Examples of storage devices.

Power Supplies

A *power supply* is a computer system component that converts line-voltage alternating current (AC) power from an electrical outlet to the low-voltage direct current (DC) power needed by other system components. The power supply is often referred to as the power supply unit (PSU). The power supply is typically a metal box in the rear of the system that is attached to the computer chassis and to the system board. While the power supply is not itself a component of the system board, it is required in order for system components to receive power. The power supply contains the power cord plug and a fan for cooling, because it generates a lot of heat. Some power supplies have a voltage selector switch that enables you to set them to the voltage configurations that are used in different countries. AC adapters are generally built in to the power supply for desktop systems and are external for laptops and other mobile systems.

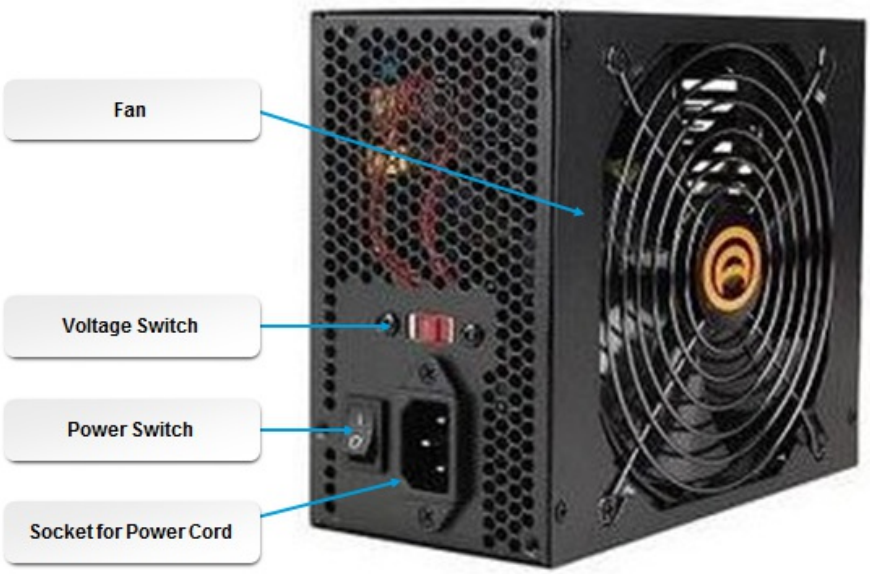


Figure: A power supply.

Fixed-Input Power Supply Voltage Selector Switch

Power supplies with voltage selector switches are called fixed-input power supplies. The voltage selector switches generally have two settings—for example, 220 and 110—depending on the manufacturer. If you set the switch to a higher voltage than supplied by the power source, the system will not receive enough power and will not function properly. However, if you set the switch to a lower setting than supplied by the power source—for example, if you set the switch to 110 volts (V) while connected to a 220 V outlet—you run the risk of burning out the power supply, damaging system components, or more seriously, creating a fire or electrocution hazard.

Auto-switching power supplies do not have a manual voltage switch, but detect the voltage level supplied by the outlet and set themselves to the correct voltage automatically. This can be convenient and safe for people who travel to various countries with portable computers.

Cooling Systems

A *cooling system* is a computer system component that prevents damage to other computer parts by dissipating the heat generated inside a computer chassis. The cooling system can consist of one or more fans and other components such as *heat sinks* or liquid cooling systems that service the entire computer as well as individual components, such as the power supply and CPU.

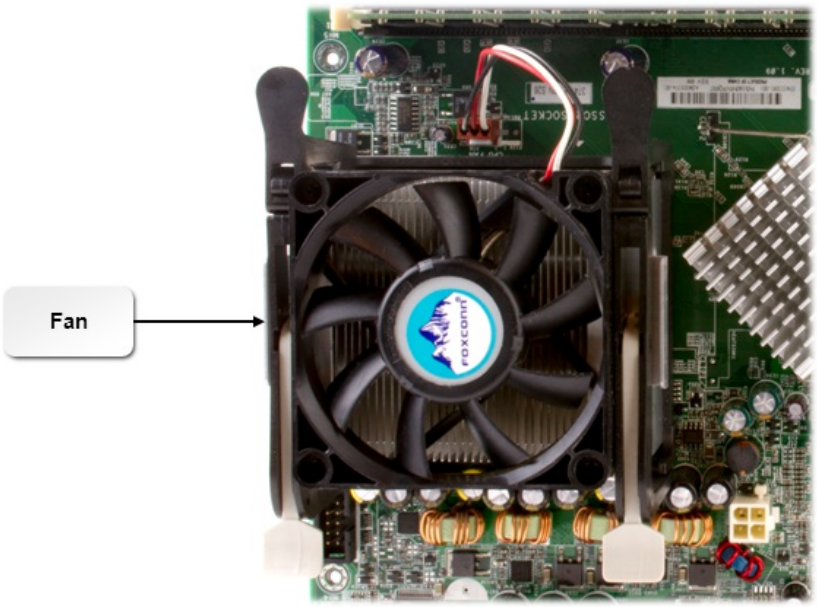


Figure: A typical cooling system for a CPU.

Components That Require Cooling

Computer systems contain several components that require cooling:

- The CPU.
- The power supply.
- Some adapter cards.
- Some hard disk drives.

Expansion Cards

An *expansion card* is a printed circuit board that you install into an expansion slot on the computer's system board to expand the functionality of the computer. In standard desktop systems, cards have connectors that fit into an expansion slot on a system board and circuitry to connect a specific device to the computer. Laptops, on the other hand, typically have slots located on the outside of the case for inserting expansion cards. These cards are often referred to as laptop expansion cards.

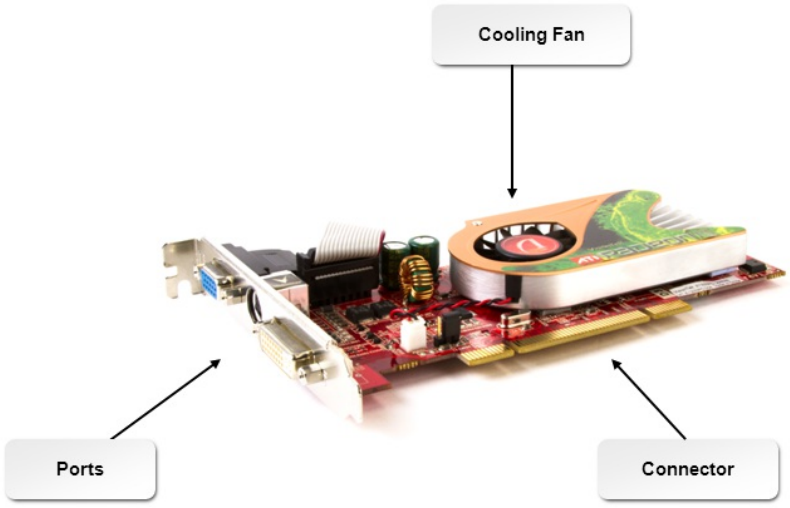


Figure: An expansion card.

Other Names for Expansion Cards

Note: An expansion card is also known as an adapter card, I/O card, add-in, add-on, or simply as a board.

Riser Cards

A *riser card* is a board that plugs into the system board and provides additional expansion slots for adapter cards. Because it rises above the system board, it enables you to connect additional adapters to the system in an orientation that is parallel to the system board and thus saves space within the system case. Riser cards are commonly found within rackmount server implementations to provide additional slots for expanding the features of a server and in low rise smaller cases to fit larger expansion cards.

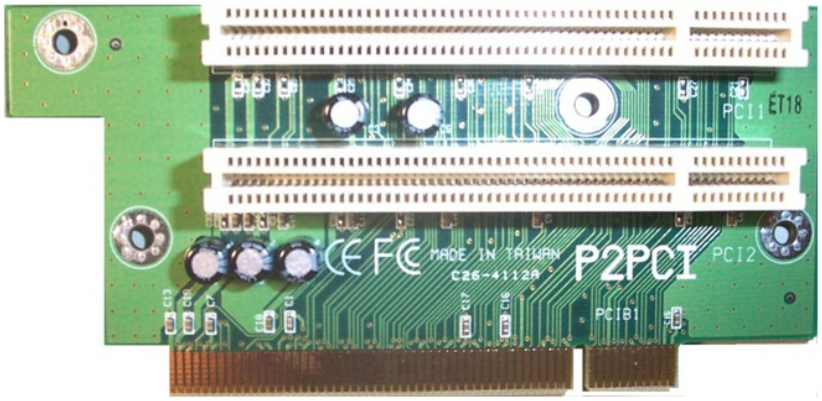


Figure: A riser card.

Riser Card and Motherboard Capabilities

Note: A riser card expands motherboard capabilities the way a power strip increases the capabilities of electrical outlets.

Daughter Boards

Daughter board is a general computing and electronics term for any circuit board that plugs into another circuit board. In personal computing, a daughter board can be used as a more general term for adapter cards. Sometimes, in casual usage, the term “daughter board” is used interchangeably with the term “riser card,” but technically they are not the same.

Firmware

Firmware is specialized software stored in memory chips that stores OS-specific information whether or not power to the computer is on. It is most often written on an electronically reprogrammable chip so that it can be updated with a special program to fix any errors that might be discovered after a computer is purchased, or to support updated hardware components.

Flashing

Note: Updating firmware electronically is called *flashing*.

The System BIOS

A *Basic Input/Output System (BIOS)* is a set of instructions that is stored in ROM and that is used to start the most basic services of a computer system. Every computer has a *system BIOS*, which sets the computer's configuration and environment when the system is powered on. It is located in ROM chips on the system board. Computers may also include other devices that have their own BIOS to control their functions.

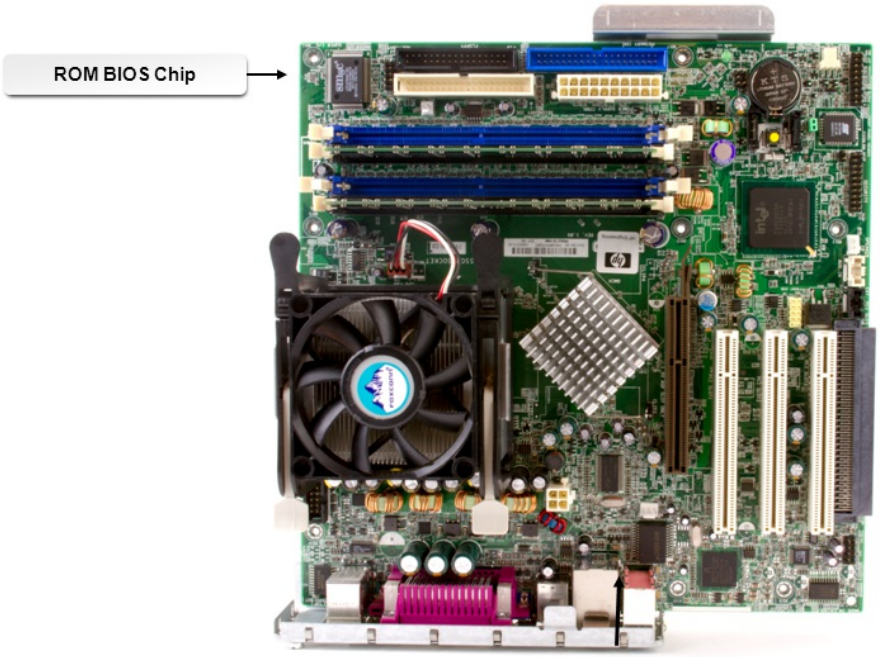


Figure: The system BIOS resides on ROM chips, and sets the computer's configuration and environment at startup.

The POST

The *Power-On Self Test (POST)* is a built-in diagnostic program that runs every time a personal computer starts up. The POST checks your hardware to ensure that everything is present and functioning properly, before the system BIOS begins the operating system boot process. If there is an error, then an audible beep will alert you that something is wrong.

The POST process contains several steps to ensure that the system meets the necessary requirements to operate properly.

POST Processes

Note: The POST process can vary a great deal from manufacturer to manufacturer.

Hardware Component	***POST Test Criteria***
Power supply	Must be turned on, and must supply its "power good" signal.
CPU	Must exit Reset status mode, and must be able to execute instructions.
BIOS	Must be readable.
BIOS memory	Must be readable.
Memory	Must be able to be read by the CPU, and the first 64 KB of memory must be able to hold the POST code.
Input/output (I/O) bus or I/O controller	Must be accessible, and must be able to communicate with the video subsystem.

ACTIVITY 1-1: Identifying Personal Computer Components

Scenario

In this activity, you will identify personal computer components.

1. Your instructor might provide you with examples of computer components and ask you or other participants to identify them.
2. **Identify the computer components in this graphic.**

A. System unit B. Display device C. Input device D. Peripheral device

3. **Which computer components are part of the system unit?**

_x_ Chassis
_x_ Internal hard drive
__ Monitor
__ Portable USB drive
_x_ Memory

4. **What are the main categories of personal computer components?**

_x_ System unit
_x_ Display
_x_ Input devices
__ Network devices
_x_ Peripheral devices

5. **Identify the system unit and motherboard components in this graphic.**

A. Motherboard B. Power supply C. Adapter card D. Storage device E. Memory F. CPU

6. **How many fans would you expect to find in a computer? How many do you think are in the computer you are using for this course?**

   A: Answers will vary, but should indicate at least one fan for the power supply. A case fan and a fan for the CPU might also be present, as well as fans on some expansion cards.

7. **Where is the system BIOS stored?**

   __ On the primary hard drive
   __ In BIOS memory
   _x_ On ROM chips
   __ In RAM

8. **Which hardware components are checked during the POST?**

   _x_ Power supply
   _x_ CPU
   __ Display
   _x_ RAM

9. **Which system unit components are connected by the system bus?**

   _x_ CPU
   _x_ Memory

__ Power supply
__ System board
__ Cooling system

Topic B: Storage Devices

In the previous topic, you identified the main components of a personal computer. One of the primary reasons for using a computer is to electronically store data. In this topic, you will identify the types of storage devices used in personal computers.

As a computer technician, your responsibilities are likely to include installing and maintaining many different types of computer components, including storage devices. By identifying the various types of storage devices that can be found in most personal computers, you will be better prepared to select, install, and maintain storage devices in personal computers.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.5: Install and configure storage devices and use appropriate media.
- Objective 1.7: Compare and contrast various connection interfaces and explain their purpose.
- Objective 1.12: Install and configure various peripheral devices.

Floppy Drives

A *floppy disk drive (FDD)* is a storage device that reads data from, and writes data to, floppy disks. Floppy disks are removable disks that are made of flexible Mylar plastic that is covered with magnetic coating and enclosed in stiff, protective plastic cases. The vast majority of floppy drives are internal devices that connect to the system board through a floppy disk *controller*, and they get their power from the personal computer's power supply. The *form factor* is usually 3.5 inches; 3.5-inch floppy disks can hold up to 1.44 MB of data. Floppy disk drives are not used much anymore and are considered a legacy technology, but you might still encounter them on older machines.

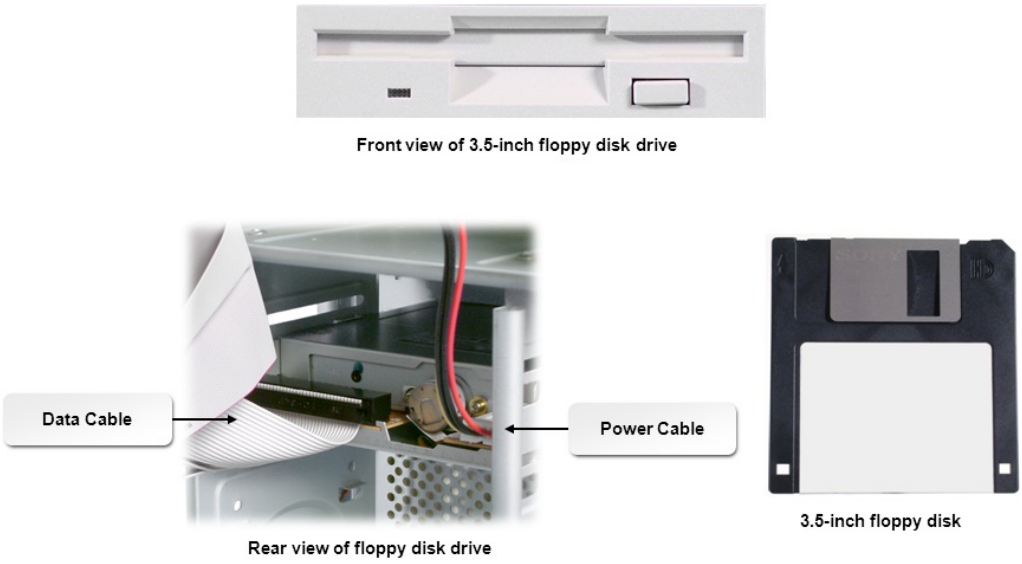


Figure: An FDD.

Note: Although 3.5 inches is the most recent standard for floppy disks and drives, 5.25-inch floppy disks and drives were once the standard, and before that, 8-inch disks and drives were the standard. You will probably never encounter either of these, and even 3.5-inch models are essentially obsolete.

Hard Drives

A *hard disk drive (HDD)* is a storage device that reads data from, and writes data to, a hard disk. A hard disk consists of several metal or hard plastic platters with a magnetic surface coating. Data is stored magnetically and can be accessed directly. Although the HDD and the hard disk are not the same thing, they are packaged together and are often referred to interchangeably. HDDs are also referred to as hard drives, and they can be internal or external devices. Internal hard drives are mounted inside the chassis and connect directly to the system board through at least one cable for data and one for power, while external hard drives generally connect to the system by means of an expansion card or a port.

Figure: An HDD.

Disk Controllers

Both floppy drives and hard drives require circuitry to communicate with the CPU. This circuitry is known as the *disk controller*. Disk controllers can be built into the drive itself, or they can be contained on an expansion card. In most modern floppy drives and hard drives, the controller is built into the drive.

Jumpers

Jumpers are used to configure older hardware by shutting off an electrical circuit located on the component. Using jumpers, this is accomplished by sliding a jumper shunt over the jumper pins on the *jumper block* of the motherboard.

Hard Drive Speeds

The speed of a hard drive is based on how fast the disk is spun to retrieve the requested data. This is referred to as revolutions per minute (rpm). Common speeds include:

- 5,400 rpm
- 7,200 rpm
- 10,000 rpm

- 15,000 rpm

Types of Hard Drives

There are many types of hard disks that you might encounter as you work with personal computers, each of which has its own set of characteristics.

Hard Drive Type	***Characteristics***
Parallel Advanced Technology Attachment (PATA)	Also known as Integrated Drive Electronics (IDE), Enhanced IDE (EIDE), Ultra Direct Memory Access (UDMA), and *Advanced Technology Attachment (ATA)* drives, PATA drives have the following characteristics: • The controller is built into the drive. • PATA drives are limited to two channels, each with up to two devices. • The earliest PATA drives came in "types," which corresponded to a particular internal geometry; the drive type needed to be set in the system BIOS. Modern drives are automatically detected. • If the drive type is not automatically detected, it must be set in the system BIOS. • Over the years, there have been several revisions to the standard, each supporting different data transfer rates. • To install PATA drives, you use jumpers to set the configuration.
Small Computer Systems Interface (SCSI)	SCSI drives have the following characteristics: • There is no controller built into the drive. A separate bus within the computer system enables SCSI drives to communicate with the CPU. • SCSI supports up to eight devices, but the host bus adapter (HBA) card installed in the computer counts as one of the devices, so you can actually connect only up to seven drives or other devices (15 devices in more recent versions). • You must configure separate SCSI ID settings for each device. • You might need to set the system BIOS to no drive, and then configure the SCSI firmware to recognize which drive to boot from. • There are several variations on the interface, each supporting different data transfer rates.

Serial Advanced Technology Attachment (SATA)	SATA drives have the following characteristics: • SATA supports one device per channel. • Data transfer rates are 150 MBps for SATA I and 300 MBps for SATA II. • SATA supports *hot swapping* of drives, which means that you can replace a SATA drive without powering down the system. • Recently, computers have started offering external SATA jacks.

PATA Configuration

Each PATA interface can support up to two drives. Because the controller is integrated with the drive, there is no overall controller to decide which device is currently communicating with the CPU. This is not a problem as long as each device is on a separate interface, but to support two devices on the same channel, the master/slave configuration was developed. This configuration allows one drive's controller (the master) to tell the other drive's controller (the slave) when it can transfer data to or from the computer. Some drives feature an option called Cable Select (CS). With the correct type of connecting cable, these drives can be automatically configured as master or slave. Most drives today come preset for CS, which allows the BIOS to configure itself as needed.

ATA and Related Specifications

Hard drive manufacturer Western Digital designed IDE technology as a replacement for even older drive technologies that did not include an integrated drive controller. American National Standards Institute's (ANSI) ATA standard was based on IDE and released in 1990. ATA referred to IBM®'s PC/AT. When SATA technology was introduced in 2003, ATA was retroactively renamed PATA.

The original IDE specification predated CD-ROM drives, and did not support hard drives larger than 504 MB. However, revisions of the specifications over the years have extended the capabilities to provide support for faster and larger hard drives and other devices. The following table describes PATA specifications.

Standard and Other Common Names for It	***Description***
IDE, ATA, ATA-1, or PATA	The original PATA specification supported one channel, with two drives configured in a master/slave arrangement. A second channel was added later.
EIDE, Fast ATA, ATA-2, or Fast ATA-2	Also known as ATA Interface with Extensions ATA-2, Western Digital called its implementation EIDE. Seagate's was called Fast ATA or Fast ATA-2. It could implement power-saving mode features, if desired.
	A minor enhancement to ATA-2, this standard improved reliability for high-speed

ATA-3	data transfer modes. Self Monitoring Analysis And Reporting Technology (SMART) was introduced. This is logic in the drives that warns of impending drive problems. Password protection was available as a security feature of the drives.
ATA/ATAPI-4, ATA-4, Ultra ATA/33, Ultra DMA, UDMA, or UDMA/33	This standard doubled data transfer rates. ATA Packet Interface (ATAPI) is an EIDE interface enhancement that includes commands used to control tape, CD-ROM, and other removable drives.
ATA/ATAPI-5, ATA-5, Ultra ATA/66, or UDMA/66	The ATA-5 specification introduced UDMA modes 3 and 4, as well as mandatory use of the 80-conductor (40-pin), high-performance IDE cable with UDMA modes higher than 2. Additional changes to the command set were also part of this specification. This standard supports drives up to 137 GB.
ATA/ATAPI-6, ATA-6, Ultra ATA/100, or UDMA/100	This standard supports data transfers at up to 100 MBps and supports drives as large as 144 petabytes (PB), which is approximately 144 million GB or 144 quadrillion bytes.
PIO	Programmed Input/Output (PIO) is a data transfer method that includes the CPU in the data path. It has been replaced by DMA and UDMA.
DMA	Direct Memory Access (DMA) is a data transfer method that moves data directly from the drive to main memory. UDMA transfers data in burst mode at a rate of 33.3 MB per second. The speed is two times faster than DMA.
SATA	This standard uses serial instead of parallel signaling technology for ATA and ATAPI devices. SATA employs serial connectors and serial cables, which are smaller, thinner, and more flexible than traditional PATA cables. Data transfer rates are 150 MB per second or greater.
SATA II, SATA2, or SATA 3 Gbps	This standard provides data transfer rates of 300 MBps.
SATA 6 Gbps	This standard doubled data transfer rates, and is designed to support the latest (and future) solid state drives (SSDs).

SCSI Standards

SCSI standards have been revised repeatedly over the years. The following table describes current SCSI standards.

SCSI Standard	***Description***
SCSI-1	Features an 8-bit parallel bus (with parity), running asynchronously at 3.5 MBps or 5 MBps in synchronous mode, and a maximum bus cable length of 6 meters, compared to the 0.45-meter limit of the PATA interface. A variation on the original standard included a *high-voltage differential (HVD)* implementation with a maximum cable length of 25 meters.

SCSI-2	Introduced the Fast SCSI and Wide SCSI variants. Fast SCSI doubled the maximum transfer rate to 10 MBps, and Wide SCSI doubled the bus width to 16 bits to reach 20 MBps. The maximum cable length was reduced to 3 meters.
SCSI-3	The first parallel SCSI devices that exceeded the SCSI-2 capabilities were simply designated SCSI-3. These devices were also known as Ultra SCSI and Fast-20 SCSI. The bus speed doubled again to 20 MBps for narrow (8-bit) systems and 40 MBps for wide (16-bit). The maximum cable length stayed at 3 meters.
Ultra-2 SCSI	This standard featured a *low-voltage differential (LVD)* bus. For this reason, Ultra-2 SCSI is sometimes referred to as LVD SCSI. LVD's greater immunity to noise allowed a maximum bus cable length of 12 meters. At the same time, the data transfer rate was increased to 80 MBps.
Ultra-3 SCSI	Also known as Ultra-160 SCSI, this version was basically an improvement on the Ultra-2 SCSI standard, in that the transfer rate was doubled once more to 160 MBps. Ultra-160 SCSI offered new features such as cyclic redundancy check (CRC), an error correcting process, and domain validation.
Ultra-320 SCSI	This standard doubled the data transfer rate to 320 MBps.
Ultra-640 SCSI	Also known as Fast-320 SCSI, Ultra-640 doubles the interface speed yet again, this time to 640 MBps. Ultra-640 pushes the limits of LVD signaling; the speed limits cable lengths drastically, making it impractical for more than one or two devices.
Serial SCSI	Four versions of SCSI—*Serial Storage Architecture (SSA), Fibre Channel-Alternating Loop (FC-AL),* IEEE 1394, and *Serial Attached SCSI (SAS)*—perform data transfer via serial communications. Serial SCSI supports faster data rates than traditional SCSI implementations, hot swapping, and improved fault isolation. *Serial SCSI* devices are generally more expensive than the equivalent parallel SCSI devices.
iSCSI	*Internet SCSI (iSCSI)* provides connectivity between SCSI storage networks over an IP-based network without the need for installing Fibre Channel.

Optical Disks

An *optical disk* is a storage device that stores data optically, rather than magnetically. The removable plastic disks have a reflective coating and require an optical drive to be read. In optical storage, data is written by either pressing or burning with a laser to create pits (recessed areas) and lands (raised areas) in the reflective surface of the disc. Common optical disks include compact discs (CDs) and digital versatile discs (DVDs).

Types of Optical Disks

There is a wide variety of optical discs available in the marketplace, each with its own requirements and specifications.

Optical Disk Type	***Description***
CD-ROM	Compact Disc-Read Only Memory. Data is permanently burned onto the disk during its manufacture.
CD-R	CD-Recordable. Data can be written to the disk only once.
CD-RW	CD-Rewritable. Data can be written to the disk multiple times.
DVD-ROM	Digital Versatile Disc-Read Only Memory. Data is permanently burned onto the disk during its manufacture.
DVD-R	DVD-Recordable. Data can be written to the disk only once.
DVD+R	Another format of DVD-Recordable. Data can be written to the disk only once.
DVD+R DL	DVD-Recordable Double Layer. A higher-capacity double-layer format. Data can be written to the disk only once.
DVD-RW	DVD-Rewritable. Data can be written to the disk multiple times.
Dual Layer DVD-RW	A DVD-RW disc that has two layer of writable space with a maximum capacity of 8.5 GB. These disks are not used widely due to the cost and the release of Blu-ray.
DVD+RW	Another format of DVD-Rewritable. Data can be written to the disk multiple times.
DVD-RAM	DVD-Random Access Memory. Data can be written to the disk multiple times.
BD-ROM	Blu-ray Disc-Read Only Memory. Blu-ray discs (BD) are intended for high-density storage of high-definition video as well as data storage. Current Blu-ray discs hold 50 GB total. However, companies such as Sony are testing experimental disks that have storage capacities of up to 200 GB and more.
BD-R	Blu-ray Disc-Recordable (BD-R). Data can be written to BD-R once.
BD-RE	Blu-ray Disc-Recordable Erasable. BD-RE is a disc that can be written to as well as erased. Data can be written to and erased from the disk many times without compromising the integrity of the disk or the data stored on it.

DVD Plus or DVD Dash?

There are several competing DVD formats. DVD-ROM, DVD-R, DVD-RW, and DVD-RAM are approved by the DVD Forum, while DVD+R, DVD+R DL, DVD+RW are not. Because some of the competing formats are incompatible, many hybrid DVD drives have been developed. These hybrid drives are often labeled DVD±RW.

Optical Drives

An *optical drive* is an internal or external disk drive that reads data to and writes data from an optical disc. Optical drives can be connected to the system by using IDE, SCSI, or other interfaces. Internal optical drives generally have a 5.25-inch form factor.

Types of Optical Drives and Burners

Optical drives include CD, DVD, and Blu-ray drives. Some optical drives provide only read capabilities, while others enable users to write, or burn, data to optical disks. CD, DVD, and Blu-ray drives have varying characteristics and specifications.

Optical Drive Type	***Description***
CD	Compact discs store data on one side of the disc, and most hold 700 to 860 MB of data, although older disks and drives may support only up to 650.4 MB of data. CDs are widely used to store music and data. To meet the audio CD standard, the CD drive on a computer must transfer data at a rate of at least 150 KBps. Most CD drives deliver higher speeds: at least eight times (8x) or sixteen times (16x) the audio transfer rate. There are also drives with much higher transfer rates, up to 52x. CD drives use one of two special file systems: Compact Disc File System (CDFS) or Universal Disc Format (UDF). CDs can be either CD-R (which can be written to once) or CD-RW (which can be written to multiple times).
DVD	Digital versatile discs can typically hold 4.7 GB on one side of the disk; it is possible to write to both surfaces of the disk, in which case the disk can hold up to 9.4 GB. There are also dual-layer disks, which store additional data on each side, and are capable of holding up to 17 GB. DVD drives access data at speeds from 600 KBps to 1.3 MBps. Because of the huge storage capacity and fast data access, DVDs are widely used to store full-length movies and other multimedia content. DVD drives use UDF as the file system. DVDs can be DVD-R (which can be written to once), or DVD-RW (which can be written to multiple times).
Blu-ray	Named for the blue laser it uses to read and write data, Blu-ray drives read and write data from Blu-ray discs. Blu-ray discs are primarily used for high-definition video, though they are also used for data storage. Blu-ray used to compete with high-definition (HD) DVD for market share, but has since emerged as the winner of that battle. The wavelength of the blue laser is shorter than that of the red laser used in previous optical drives, so data can be more tightly packed on a Blu-ray disc. A single-layer Blu-ray disc can hold up to 25 GB of information, and a dual-layer Blu-ray disc can hold up to 50 GB, dwarfing the capacity of a standard double-sided DVD. Blu-ray uses UDF v2.5.
	A combination drive, also referred to as a combo drive, can read and write to a number of different optical disc types. Older combo drives were equipped with the read/write function for CDs only, but could also read DVDs. However, most combo drives today

Combination drives and burners	are primarily DVD-RW burners that also have the ability to read/write CDs and Blu-ray discs. Depending on your needs, you may require a combo drive that can also support the use of dual-layer DVD-RW discs. Depending on the manufacturer, some combination Blu-ray drives and players can also read/write to CDs and DVDs. It is a best practice to check the specific manufacturer's drive capabilities to verify which media the device can support.

Tape Drives

A *tape drive* is a storage device that stores data magnetically on a tape that is enclosed in a removable tape cartridge. Data on the tape must be read sequentially. Sizes for external tape drives vary, but internal drives have a 5.25-inch form factor. Tape drives are most commonly used to store backup copies of archived, offline data in large data centers and are almost never used with desktop computers. Recent technological advances made by IBM have allowed for data on tapes to be accessed and read in a file format method similar to other storage media, such as optical disks and flash drives. The specification is called *Linear Tape File Systems (LTFS)*. LTFS is a tape format that determines how data is recorded on tape, and how specialized software will read that data.

Figure: A tape drive.

Solid State Storage

Solid state drives (SSDs), use flash technology to retain data in special types of memory instead of on disks or tape. Solid state storage uses non-volatile memory to emulate mechanical storage devices, but solid state storage is much faster and more reliable than mechanical storage because there are no moving parts.

Solid State vs. Magnetic Storage

Storage devices typically store data in either solid state or magnetic form. Solid state devices, such as *flash drives,* contain no moving parts and tend to be more reliable than magnetic drives. Magnetic drives, such as hard drives, store information on a magnetic coated media that is rotated underneath a read/write head.

Hot Swappable Devices

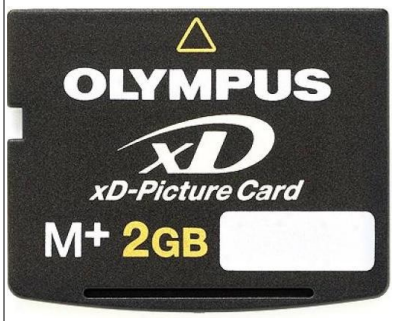
Hot swapping is a type of hardware replacement procedure where a component can be replaced while the main power is still on. Also called hot plug or hot insertion, hot swap is a feature of USB and FireWire devices, enabling you to install an external drive, network adapter, or other peripheral without having to power down the computer. It is good practice to use the safe removal option from the System Tray before removing a hot-swappable device or peripheral from the computer. Hot swapping can also refer to the system's ability to detect when hardware is added or removed. Non-hot-swappable devices require the system to be shut down and restarted before any device installation updates or removals are recognized by the system.

Types of Solid State Storage

Solid state storage comes in several formats, many of which are used in external devices such as digital cameras or mobile devices.

Solid State Storage Device	***Specifications***
USB flash drives	USB flash drives come in several form factors, including thumb drives and pen drives. Thumb drives can be small, from 50 to 70 mm long, 17 to 20 mm wide, and 10 to 12 mm thick. Data storage capacities vary, from 128 MB up to 128 GB. Data transfer rates also vary, from 700 KBps to 28 MBps for read operations, and from 350 KBps to 15 MBps for write operations.
SSDs	Flash-memory-based disks do not need batteries, allowing makers to replicate standard disk-drive form factors (2.5-inch and 3.5-inch). Flash SSDs are extremely fast since these devices have no moving parts, eliminating seek time, latency, and other electromechanical delays inherent in conventional disk drives. The use of SSDs has been increasing over time due to their speed and quick data access times. SSDs can be configured within systems to replace traditional computer hardware such as disk drives, optical drives, and network security appliances that include firewall and routing functions.

CF cards	CompactFlash (CF) cards are flash memory cards that are 43 mm long by 36 mm wide. Due to their compact size, they are typically used in portable devices. Type I is 3.3 mm thick and Type II is 5 mm thick. They hold 100 GB or more, and have a 50-pin contact. Transfer speeds of up to 66 MBps are possible. Newer versions of the CF card offer speeds up to 1 Gbps and can store up to 1 terabyte (TB) of data. CF cards are commonly used for additional storage in: • Digital cameras • Music players • Personal computing devices • Photo printers • Digital camera recorders
SM	SmartMedia (SM) cards are flash memory cards that are similar in size to the CF cards, and are 45 mm long by 37 mm wide by 0.76 mm thick. They can hold up to 128 MB and can transfer data at speeds of up to 8 MBps. SM cards are commonly used for additional storage in: • Digital cameras • Digital camera recorders • Older models of personal digital assistants (PDAs)

cards	
xD	xD-Picture Cards (xD) are flash memory cards that are specifically designed for use in digital cameras. They are 20 mm long by 25 mm wide by 1.7 mm thick. They can hold up to 2 GB with plans for up to 8 GB. Data transfer rates range from 4 to 15 MBps for read operations and from 1.3 to 9 MBps for write operations. 
MSes	Memory sticks (MSes) are flash memory cards that are 50 mm long by 21.5 mm wide by 2.8 mm thick. They can hold up to 16 GB and are used extensively in Sony products such as VAIO® laptops. Data transfer rates are 2.5 MBps for read operations and 1.8 MBps for write operations.
	The original Secure Digital (SD) Memory Card is 32 mm long, 24 mm wide, and 2.1 mm thick. The miniSD Card measures 21.5 mm by 20 mm by 1.4 mm, and the microSD/TransFlash Card measures 15 mm by 11 mm by 1 mm. SD Memory Cards are currently available in several capacities, up to 2 TB. Data transfer rates range from 10

SD cards	MBps to 20 MBps. SD cards are used in many different devices, including: • Laptops • Digital cameras • Smartphones • Handheld gaming devices • Audio players
MMCs	MultiMediaCards (MMCs) are 32 mm long by 24 mm wide by 1.5 mm thick. Reduced Size MMCs (RS-MMCs) and MMCmobile cards are 16 mm by 24 mm by 1.5 mm. MMCmini cards are 21.5 mm by 20 mm by 1.4 mm, and MMCmicro cards are 12 mm by 14 mm by 1.1 mm. These cards can hold up to 8 GB, and data transfer rates can reach 52 MBps. MMC cards are generally also compatible with SD card readers and are used in many of the same devices.

ACTIVITY 1-2: Identifying Storage Devices

Scenario

In this activity, you will identify storage devices.

1. Your instructor might provide you with examples of storage devices and ask you or other participants to identify them.

2. **Which storage device records data magnetically and is most often used for backups?**

   __ FDD
   __ HDD
   __ Optical disk drive
   _x_ Tape drive
   __ SSD

3. **What is the primary benefit of using solid state storage?**

   A: Answers will vary, but should include the portability of thumb drives and other small solid state devices, and the speed of data access when compared to traditional magnetic storage media.

4. **Which two optical drive media types enable you to write to an optical disk only once?**

   __ CD-ROM
   _x_ CD-R
   __ CD+RW
   _x_ DVD+R
   __ DVD-RW

5. **True or False? No optical disk can hold more than 50 GB of data.**

   __ True
   _x_ False

Topic C: Device Connections and Interfaces

You are already familiar with the common components that make up a personal computer. Next, you need to be able to identify how all the components are connected together to form a complete personal computer system. In this topic, you will identify device connection and interface methods.

A personal computer is made up of many different components. All of these components need to be able to communicate with each other in order for the computer to function properly. As personal computers have evolved over the years, a number of connection technologies have been implemented to provide communication among computer components. As a computer technician, identifying the different methods that are used to connect devices to a computer will enable you to install, upgrade, and replace personal computer components quickly and effectively.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.7: Compare and contrast various connection interfaces and explain their purpose.
- Objective 1.11: Identify connector types and associated cables.

Ports

A *port* is a hardware interface that you can use to connect devices to a computer. The port transfers electronic signals between the device and the system unit. The port is either an electrically wired socket or plug, or it can be a wireless transmission device. Ports can vary by shape, by color according to the color coding standards, by the number and layout of the pins or connectors contained within the port, by the signals the port carries, and by the port's location. Ports exist for both internal and external devices. External ports often have a graphical representation of the type of device that should be connected to it, such as a small picture of a monitor adjacent to the video port.

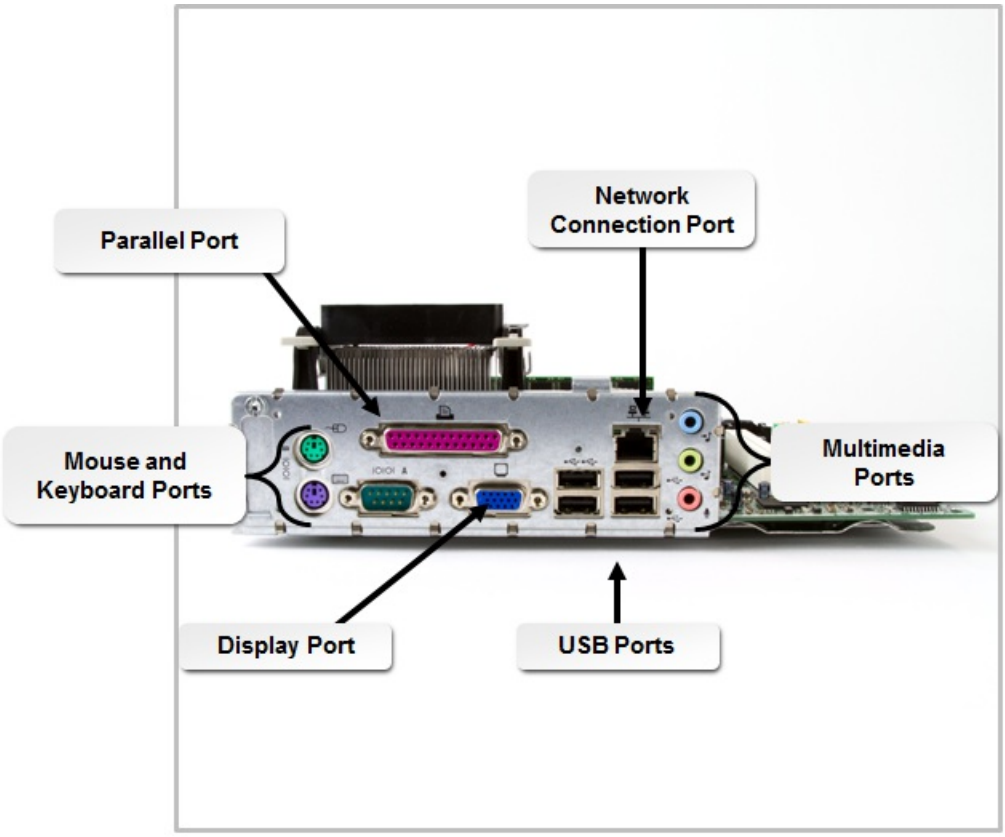


Figure: Ports on a personal computer.

Genders

Most ports and the cables that connect to them have genders. For example, most computer ports are jacks, into which you plug in the matching cable. The computer's jacks are most often the female connectors and the cable's plug is most often the male connector. You can always look directly at the innermost electrical connections on the connectors to determine the gender. The one with the protruding pins is the male and the one with the holes to accept the pins is the female.

Port Shapes

Ports can have different physical shapes such as round, rectangular, square, and oblong. There is some standardization of physical properties and functions, though. Most connectors are keyed in some

way to restrict connecting devices into the wrong port.

PS/2 Ports

The round 6-pin port, also referred to as a mini-Din connector or PS/2 port, is an interface located on the motherboard. The Din-6 port is the larger 13.2 mm port. Many keyboards and mice use PS/2 ports to connect to the motherboard. To avoid confusion between the identical-looking keyboard and mouse ports, PS/2 ports are often color-coded to match the end of the cable on the device: purple for the keyboard and green for the mouse. Or, there may be a sticker with a picture of a mouse and keyboard near the connectors.

Computer Connections

Computer connections are the physical access points that enable a computer to communicate with internal or external devices. They include the ports on both the computer and the connected devices, plus a transmission medium, which is either a cable with connectors at each end or a wireless technology. Personal computer connections can be categorized by the technology or standard that was used to develop the device.

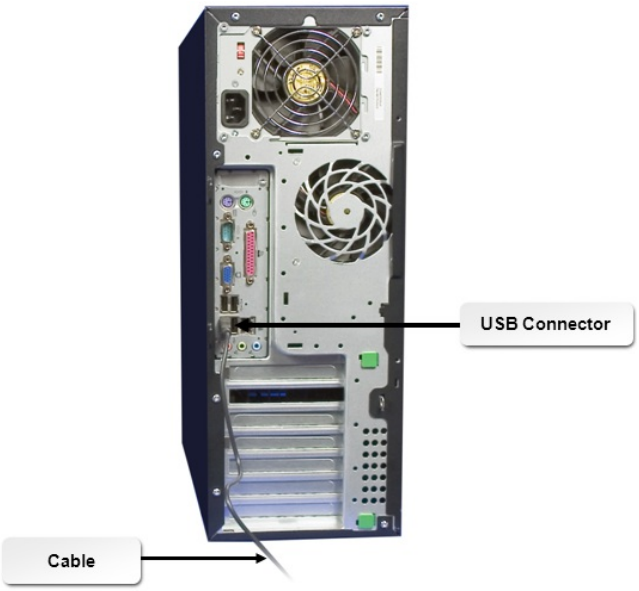


Figure: A personal computer connection.

Serial Connections

A *serial connection* is a personal computer connection that transfers data one bit at a time over a single wire. Serial connections support two-way communications and were typically used for devices such as fax cards or external modems. These legacy serial ports have either 9-pin (DB-9) or 25-pin (DB-25) male connectors. A legacy serial cable ends with a female connector to plug into the male connector on the system unit. On system units that have color-coded ports, the serial port is teal-colored. Serial connections that are seen today are used to attach printers, scientific devices such as telescopes, networking hardware such as routers and switches, and industrial products. In most cases, these devices will need to be connected using a USB adapter.

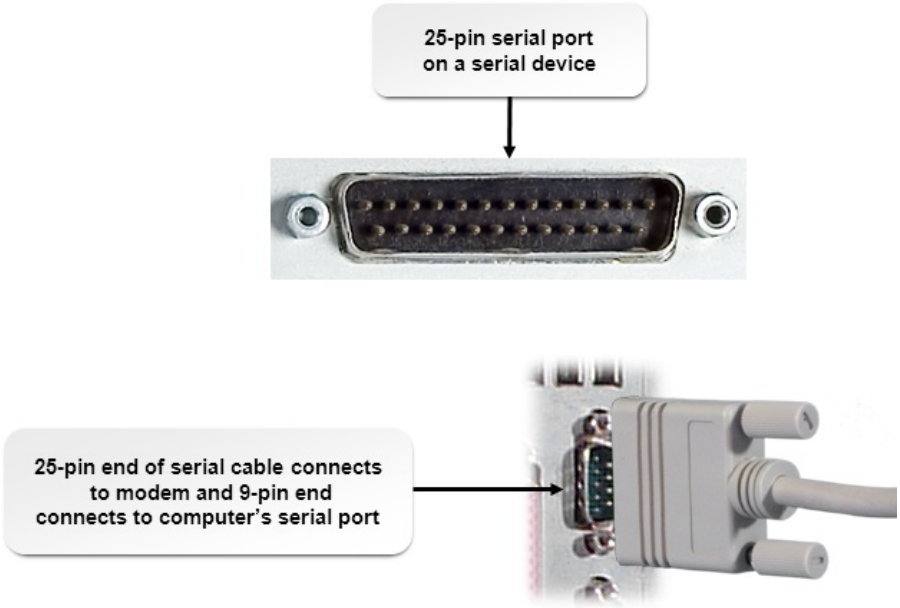

25-pin serial port
on a serial device
25-pin end of serial cable connects
to modem and 9-pin end
connects to computer's serial port

Figure: A serial connection.

Serial Transmissions

In a serial transmission, data is sent and received one bit at a time over a single wire. To accomplish this, the serial communication process:

1. Disassembles bytes into bits on the sending end of the communication.
2. Sends the bits across the communication wires.
3. Reassembles the bits into bytes at the receiving end.

Serial Port Naming

Serial ports are typically called COM1, COM2, COM3, and COM4, where "COM" is short for communications port. This port has been almost completely phased out in favor of USB. You'll probably find many systems with no serial ports at all.

Parallel Connections

A *parallel connection* is a computer connection that transfers data eight or more bits at a time over eight or more wires. Any components connected by multiple data pathways may be considered to have a parallel connection, but the term is generally used to refer to a standard legacy parallel port that uses eight data wires, and is typically used to connect a printer to a system unit. Parallel connections in older personal computers support only one-way or unidirectional communications. Newer computers have parallel ports that support bidirectional communications. Standard parallel ports have 25-pin female connectors. A parallel cable has a 25-pin male connector to plug into the system unit and a 36-pin male Centronics connector at the other end to attach to the external device. On system units that have color-coded ports, the parallel port is burgundy or dark pink.

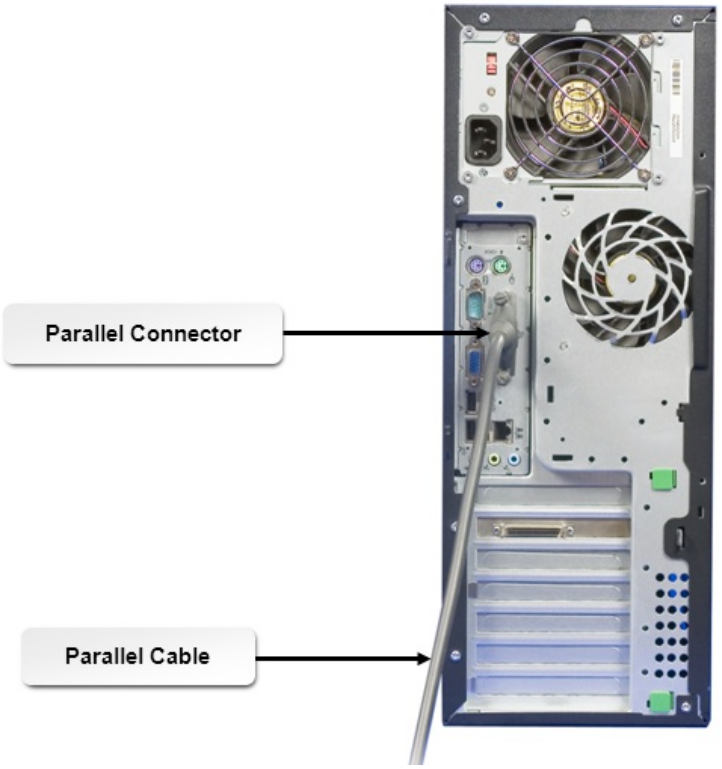


Figure: A parallel connection.

Note: The standard parallel port has been phased out in favor of USB, so you may find many systems with no parallel ports at all.

FDD Connections

Internal FDDs have two primary connections: the power connection and the data connection. The data connection is a parallel connection. The FDD cable is a 34-pin flat ribbon cable with a twist, which is used to differentiate between multiple FDDs in a system.

USB Connections

A *universal serial bus (USB) connection* is a computer connection that enables you to connect multiple peripherals to a single port with high performance and minimal device configuration. USB connections support two-way communications. All modern PC systems today have multiple USB ports and can, with the use of USB hubs, support up to 127 devices per port. USB cables may have different connectors at each end. The computer end of the cable ends in a Type A connector. The device end of the cable commonly ends in a Type B connector, or may also end in a Mini-A, Mini-B, Micro-AB, or Micro-B connector. The mini connectors are typically used for portable devices such as smartphones. The size of the connector varies depending on the device. USB connections transfer data serially, but at a much faster throughput than legacy serial connections. USB devices also incorporate Plug-and-Play technology that allows devices to self-configure as soon as a connection is made.

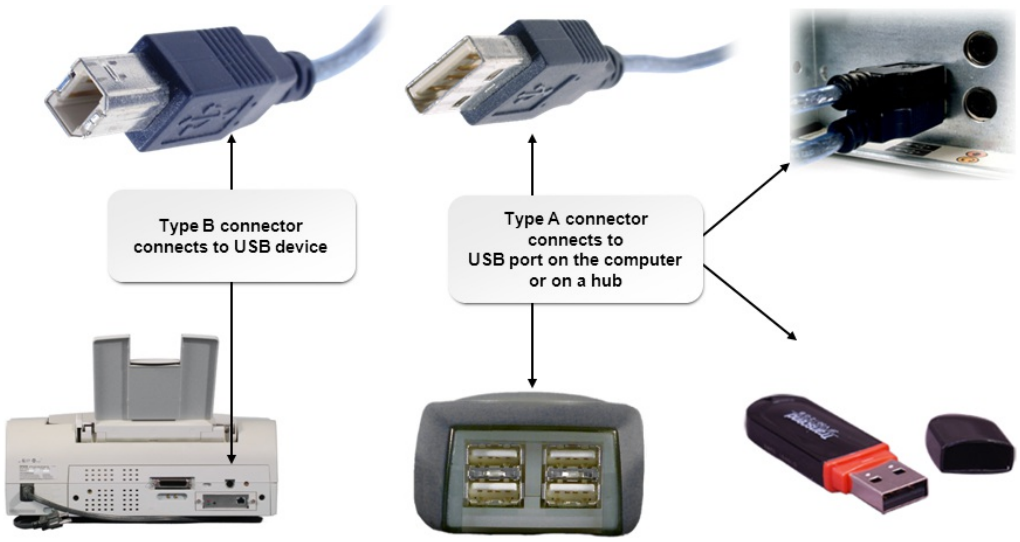


Figure: USB connections.

USB Standards

USB 2.0, released in April 2000, is the most commonly implemented standard. It can communicate at up to 480 Mbps. The original USB 1.1 standard is still commonly found in devices and systems. It can communicate at up to 12 Mbps. A USB 2.0 device connected to a USB 1.1 hub or port will communicate at only USB 1.1 speeds, even though it might be capable of faster speeds. Generally, the operating system will inform you of this when you connect the device.

USB 3.0, also called SuperSpeed USB, is the latest USB standard released in November 2008. It features a maximum transfer rate of 5.0 Gbps. It is 10 times faster than the USB 2.0 standard, has enhanced power efficiency, and is backward compatible with USB-enabled devices currently in use.

USB cables have a maximum distance before performance suffers. To work around this, one or more hubs can be used to create a "chain" to reach the necessary cable length. USB 1.1 has a maximum cable length of 3 meters, while USB 2.0's maximum length is 5 meters. In each case, a maximum of

five hubs can be used to extend the cable length. The maximum cable length is not specified in the USB 3.0 specification.

IEEE 1394 and FireWire Connections

A *FireWire connection* is a computer connection that provides a high-speed interface for peripheral devices that are designed to use the *Institute of Electrical and Electronic Engineers (IEEE)* 1394 standard. FireWire can support up to 63 devices on one FireWire port. FireWire 400 transmits at 400 Mbps and uses either a 6-pin, bullet-shaped, powered connector or a 4-pin square-shaped, unpowered, connector. FireWire 800 transmits at 800 Mbps and uses a 9-pin connector.

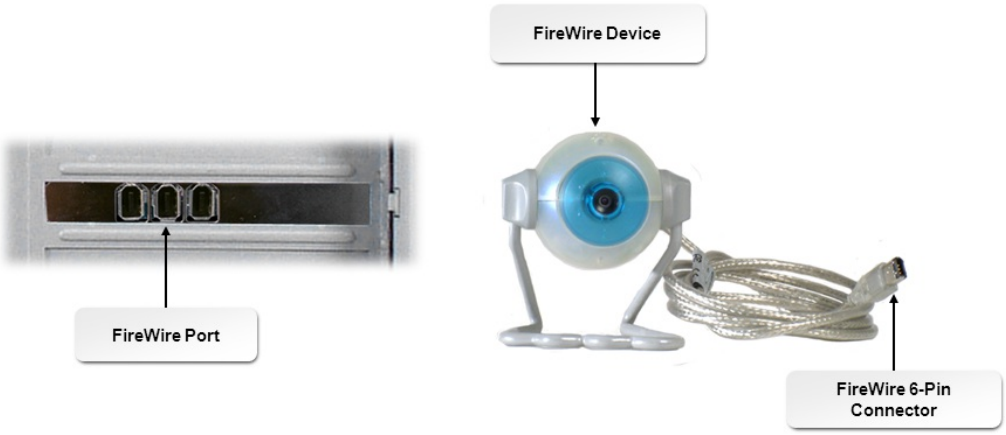


Figure: A FireWire connection.

FireWire Terminology

Apple® was the primary vendor to promote the IEEE 1394 Standard, and used the FireWire name as a trademark for the IEEE 1394 implementation included in its Macintosh® systems. FireWire has since become the common name for all IEEE 1394 devices.

FireWire vs. USB

FireWire predated USB and was faster than the original USB 1.1 standard. USB 2.0, with its increased speed, largely superseded FireWire. However, although USB 2.0 is faster by the numbers than FireWire, FireWire is actually faster on throughput, making it ideal for video/audio file transfers and external storage devices. A file transfer of 100 separate documents might be slightly faster on USB than FireWire, but a file transfer of a single 2 GB video file will be much faster in FireWire. Also, while USB provides a device up to 5 V power, FireWire provides up to 12 V power on the wire.

With the release of USB 3.0 and the latest FireWire S3200, the performance will still vary. USB 3.0 is 10 times faster than USB 2.0, and will remain the popular standard used for most devices. The FireWire S3200 standard, however, still has considerable advantages over USB. For example, FireWire uses much less CPU power, and provides more power over a single cable connection.

Similar to USB, FireWire has maximum distance restrictions. However, FireWire's distances are greater than USB's. A FireWire "chain," created with cables and repeaters, can reach up to 237 feet

from device to host, while USB 2.0 can reach 30 meters (just under 100 feet).

SCSI Connections

SCSI, pronounced “scuzzy,” is an older connection standard, typically used for storage devices such as tape and hard drives, that remains in use due to its reliability and high speed. A SCSI adapter has a port for external devices and a connection for internal devices. SCSI devices themselves can have multiple ports, enabling you to connect up to seven devices in a chain to one SCSI adapter. Each device in the chain requires a unique ID, which you configure by using switches or jumpers. SCSI cables have 25-pin, 50-pin, 68-pin, or 80-pin connectors, depending upon the type of SCSI in use.

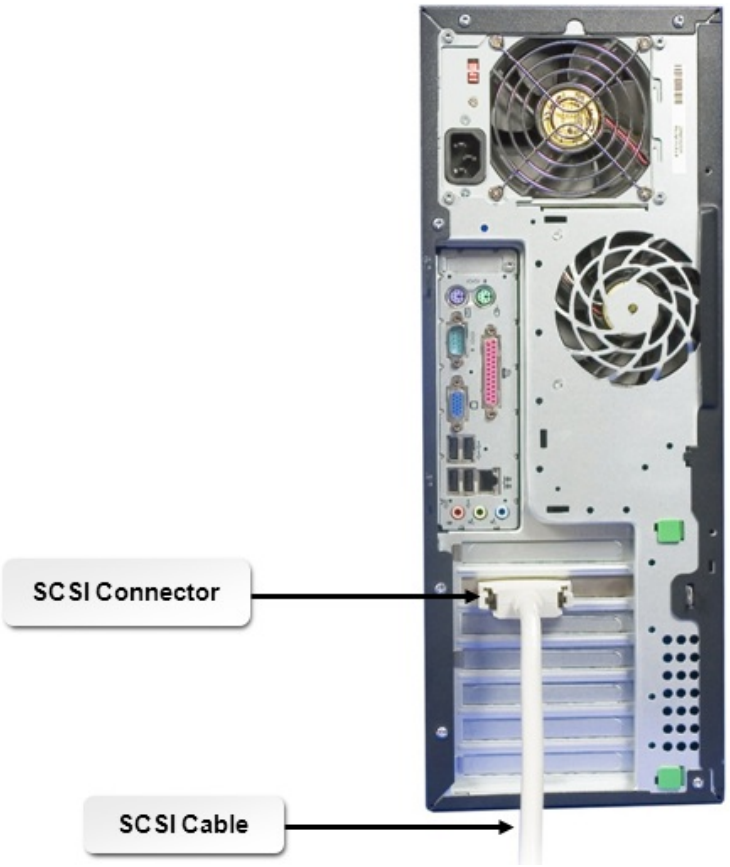


Figure: A SCSI connection.

PATA Connections

A PATA connection is a drive connection standard that provides a parallel data channel from the drive controller to the disk drives. Originally called ATA, IDE, EIDE, or UDMA, PATA connections are used to connect internal hard drives, optical drives, and tape drives to the system board. On the system board, two sockets provide connections for up to two drives per socket. PATA cables are ribbon cables with 40 or 80 wires and 40-pin connectors.

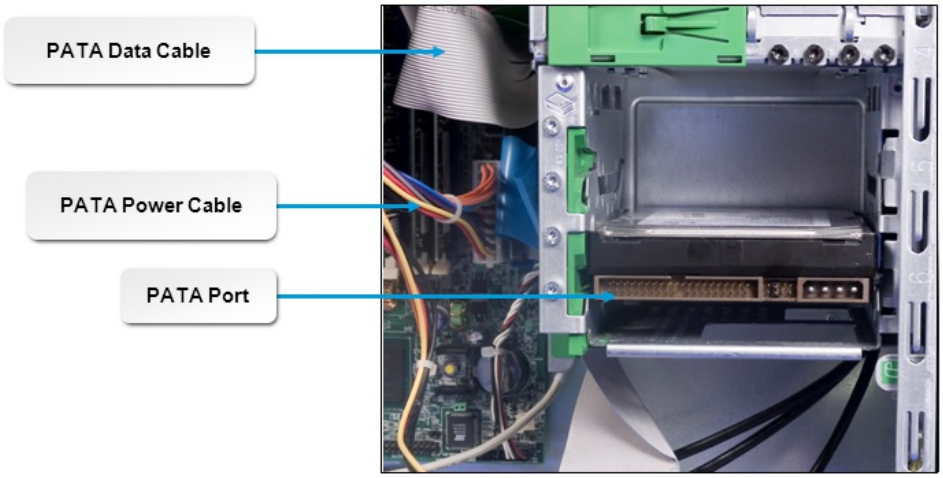


Figure: A PATA connection.

Pronunciation

Note: You might hear PATA pronounced “Parallel ay-tee-ay,” “PEE-ay-tee-ay,” “PAY-tuh,” or “PAT-uh.”

ATA, IDE, EIDE, and UDMA

IDE, EIDE, and UDMA are alternative names for the ATA standards that are now referred to as PATA. (After Serial ATA drives became popular, the PATA term was coined to refer to the parallel drives.) There have been several versions of the ATA standard, with successive versions providing support for different types of devices, or providing performance enhancements such as higher data rates. For example, ATAPI provides support for tape drives and CD-ROM drives, while ATA-7 supports data rates up to 133 Mbps.

Master and Slave Designations

PATA drives are configured in a master/slave hierarchy, usually by setting jumpers. Each PATA channel can support one or two devices. Because each PATA device contains its own integrated controller, you need to have some way of differentiating between the two devices. This is done by giving each device a designation as either master or slave, or by using the Cable Select (CS) feature to assign master and slave designations, and then having the controller address commands and data to

either one or the other.

Scheme	Description
Master/slave	In the master/slave configuration scheme, the drive that is the target of the command responds to it, and the other one ignores the command, remaining silent. Each manufacturer uses a different combination of jumpers for specifying whether its drive is master or slave on the channel, though they are all similar. Some manufacturers put this information right on the top label of the drive itself, while others do not. Jumper information is available in the hard disk's documentation, or by checking the manufacturer's website and searching for the model number.
CS	With CS, you do not have to set jumpers to designate which device is master and which is slave. The connectors that are connected to the devices take care of the configuration. To set up CS, you need to use a jumper to set both devices on the channel to the CS setting, along with a special cable. This cable is similar in most respects to the regular PATA cable, except for the Cable SELect (CSEL) signal, which the devices use to determine which is the master and which is the slave.

SATA Connections

A SATA connection is a drive connection standard that enhances PATA by providing a serial data channel between the drive controller and the disk drives. SATA transfer speeds are much higher than PATA for the same drive technologies. SATA's physical installation is also easier because the SATA power and data cables are much smaller, thinner, and more flexible than traditional PATA ribbon cables. SATA connectors have seven pins.

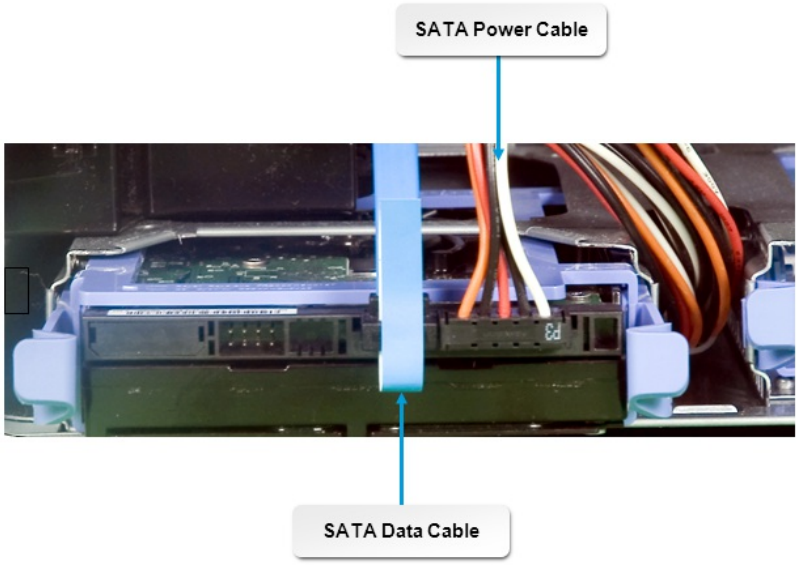


Figure: A SATA connection.

Note: You might hear SATA pronounced “Serial ay-tee-ay,” “ESS-ay-tee-ay,” “SAY-tuh,” or “SAT-uh.”

Note: Although current practice is to use the terms “IDE” and “PATA” interchangeably, you should be aware that SATA is also a type of IDE drive, but with a different interface.

eSATA

External SATA (eSATA) is an external interface for SATA connections. Like USB and FireWire, it provides a connection for external storage devices. eSATA connections provide fast data transfers without having to translate data between the device and the host computer. eSATA interfaces do require an additional power connector to function. You can provide eSATA functionality by installing eSATA cards in systems.

Display Cable and Connector Types

Display devices can use several different types of cables.

Cable Type	*Description*
Video Graphics Array (VGA)	The *DB-15* high-density VGA connector is the most common cable used for LCD monitors. It contains three rows of five pins. Pins 4, 11, 12, and 15 receive information from the device, while pins 1, 2, 3, 13, and 14 send information to the display. Mini-VGA is used on smaller devices, such as laptops, in place of the standard full-sized cables.
Digital Video Interface (DVI)	DVI cables keep data in digital form from the computer to the display. There is no need to convert data from digital information to analog information. LCD monitors work in a digital mode and support the DVI format. • DVI-analog (DVI-A) is an analog-only format. It requires a DVI-A supported interface. The connector does not support dual link technology. It is commonly used to connect CRT or VGA devices to a computer using a DVI-A adapter. • DVI-digital (DVI-D) is a digital-only format. It requires a video adapter with a DVI-D connection and a monitor with a DVI-D interface. The connector contains 24 pins/receptacles in three rows of eight above or below a flat blade, plus a grounding slot for dual-link support. For single-link support, the connector contains 18 pins/receptacles. • DVI-integrated (DVI-I) supports both digital and analog transmissions. This gives you the option to connect a monitor that accepts digital input or analog input. In addition to the pins/receptacles found on the DVI-D connector for digital support, a DVI-I connector has four additional pins/receptacles to carry an analog signal. For single-link support, the connector contains 18 pins/receptacles, and four additional pins for analog transmissions.

High Definition Multimedia Interface (HDMI)	HDMI is the first industry-supported uncompressed, all-digital audio/video interface. HDMI uses a single cable composed of copper wires to provide an interface between any audio/video source, such as a set-top box, DVD player, or A/V receiver and an audio and/or video monitor, such as a digital television (DTV). The connector is made up of 19 pins and can support a number of modes such as High Definition TV (HDTV), Standard Definition TV (SDTV), and Enhanced Digital TV (EDTV) can run to 50 feet or more in length. HDMI has largely superseded DVI and is compatible with the DVI standard. It can be used with PC systems that support DVI.
Mini-High Definition Multimedia Interface (Mini-HDMI)	Mini-HDMI is similar to the full size HDMI connector, except that it is specified for use with portable devices. The connector is a smaller version of the full size with same number of pins. The difference between the full size and the mini is that some of pins have different transmission functions.
	S-Video is an analog video signal that carries the video data as two separate signals (brightness and color). S-Video works in 480i or 576i resolution.

Separate Video (S-Video)	**Note:** Video resolution is sometimes noted in the format shown here, particularly when television signals are being discussed. A resolution of 480i indicates a vertical frame resolution of 480 interlaced lines that contain picture information, while a resolution of 576i indicates a vertical frame resolution of 576 interlaced lines that contain picture information.
Component/RGB	Component video is a type of analog video information that is transmitted or stored as two or more separate signals. Analog video signals (also called components) must provide information about the amount of red, green, and blue to create an image. The simplest type, RGB, consists of three discrete red, green, and blue signals sent down three coaxial cables.
Composite video	Composite video is the format of an analog (picture only) signal before it is combined with a sound signal and modulated onto a radio frequency (RF) carrier.
Coaxial	A coaxial cable, or coax, is a type of copper cable that features a central conducting copper core surrounded by an insulator and braided or foil shielding. An insulator separates the conductor and shield, and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

DisplayPort	DisplayPort is a digital display standard that aims to replace DVI and VGA standards. DisplayPort is not backward compatible with DVI and HDMI and is a royalty-free standard. However, by using special dual-mode ports and suitable adapters, it may be possible to use DVI and HDMI signals with DisplayPort. Similar to Peripheral Component Interconnect Express (PCIe), DisplayPort also supports high-quality gaming and other applications that use high-end graphics.
Radio Corporation of America (RCA)	RCA cables and connectors are used to carry audio and video transmissions to and from a variety devices such as TVs, digital cameras, and gaming systems. In some cases, the RCA cable may also be used as a power cable, a loud speaker cable, and to carry digital audio. The female jacks on the devices are colored to provide a guide as to what type of connector can be attached. Common colors found are: • Yellow for various composite connections. • Red for the right channel of the audio transmission. • White or black for the left channel of audio transmission.
	The BNC connector is used with coaxial cable to carry radio frequencies to and from devices. The BNC cable can be used to connect radio equipment, aviation electronics, and to carry video signals. The actual BNC connectors come in two

Bayonet Neill-Concelman (BNC)	versions. The connector will be either 50 or 75 ohms, depending on the specific cable that is attached.

Ethernet and Displays

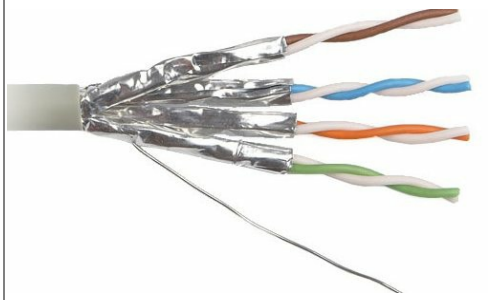
Some display devices such as the Apple Thunderbolt display include an Ethernet port for connection directly to a network.

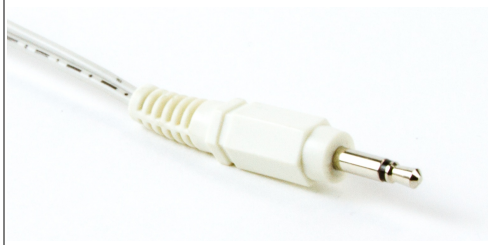
DVI Single Link vs. Dual Link

DVI cables use a technology called Transition Minimized Differential Signaling (TMDS) to transmit serial data over a high-speed connection. Single link cables use a single TMDS transmitter to carry data, while double-link uses two. Therefore, dual link cables can transmit larger images at higher speeds than single link.

Audio/Video Connections

There are a number of audio/video connectors that are used to connect a wide variety of devices, including PCs, DVD and Blu-ray players, surround sound systems, stereo equipment, projectors, and HDTVs. In addition to HDMI and DVI, common audio/video cable and connectors include those described in the following table.

Type	*Description*
Single-core/shielded cable	The single core wire is the positive, and the shield is the negative. This type of cable is used for unbalanced audio signals. Generally, unbalanced audio cables are short, because noise is less of an issue.
One pair/shielded cable	Uses a pair (white and red) of cores with one wire being the positive, and the other wire being the negative. The shield acts as a ground. This type of cable is used for balanced audio signals. Balanced audio is a method for minimizing noise and interference in audio cables. 
	The most common connectors used in for unbalanced audio cables are the 1/4-inch tip-sleeve (TS) or tip-ring-sleeve (TRS) and RCA connectors, which are typically used with high-end audio equipment. The 1/8-inch tip-sleeve is typically used with smaller audio devices such as Apple® iPods®. TS and TRS connectors are also referred to as phone jacks, phone plugs, audio jacks, and jack plugs. Traditionally, TS connectors are used for mono, while TRS connectors are used for stereo. Some connectors can carry more signals; these are often used with camcorder, laptops, and other devices. Stereo connectors can also carry a single, balanced signal. Wiring configurations for TRS connectors include:

TS and TRS connectors	• For unbalanced mono, the tip carries the signal, the ring is not connected, and the sleeve acts as ground. • For balanced mono, the tip is positive, the ring is negative, and the sleeve acts as ground. • For stereo, the tip carries the left channel, the ring carries the right channel, and the sleeve acts as ground. 
3-pin XLR connectors	The standard connector for balanced audio is the 3-pin XLR. The most common wiring configuration is: • Pin 1: Shield (ground) • Pin 2: Positive (hot) • Pin 3: Negative (cold)

Analog vs. Digital Video

Analog transmissions carry information in the form of a continuous wave. Analog signals are most often generated by electrical current, the intensity of which is measured in volts. An analog signal oscillates over time between maximum and minimum values and can take on any value between those limits. The size, shape, and other characteristics of that *waveform* describe the analog signal and the information it carries. *Digital transmissions*, unlike analog transmissions, which can have many possible values, hold just two values—ones and zeroes. These values represent an on and off state, respectively. Digital data, which is a sequence of ones and zeroes, can be translated into a digital waveform. In computer systems and other digital devices, a waveform switches between two voltage levels representing 0 and 1.

VGA vs. HDMI

VGA and HDMI are inherently different because one is analog (VGA) and the other is digital (HDMI). Many home theater environments will use one or the other, or in some cases both, if an adapter is applied. Traditional VGA has a maximum resolution of 800 by 600 pixels and Super VGA (SVGA) has a resolution up to 2,048 by 1,536 pixels or more, while the latest version of HDMI 4.1 has the capability of carrying a resolution up to 4,196 by 2,160 pixels.

Wireless Device Connections

Wireless is rapidly becoming the primary connection method for connecting a wide variety of computer components, as well as for connecting computing devices to each other. There are a number of connection methods you can use to accomplish this.

Connection Method	***Description***
Radio frequency (RF)	*Radio networking* is a form of wireless communication in which signals are sent via RF waves, in the 10 KHz to 1 GHz range, to wireless antennas. An antenna transmits by converting electrical energy into an RF wave. When an antenna receives a transmission, it converts the RF wave into electrical energy. In wireless communication, low-frequency data or voice signals are transmitted through high-frequency radio waves by superimposing data on them.
Bluetooth	Bluetooth® is a wireless technology that facilitates short-range wireless communication between devices, such as personal computers and some of their components, laptops and some of their components, mobile phones, and gaming consoles and other gaming peripherals. Both voice and data information are exchanged among these devices at 2.4 GHz within a range of approximately 30 feet. A maximum of eight Bluetooth devices can be connected to each other at a time; this connection of two to eight Bluetooth-enabled devices is known as a *piconet*. Bluetooth devices operate at very low power levels of approximately 1 milliwatt (mW). Bluetooth is predominantly used in wireless personal area networks to transfer information between two computers or other devices. It is also used in mobile headsets for communicating with mobile phones. Computer peripherals such as the mouse, keyboard, and printer can also use Bluetooth for communication. Bluetooth-enabled devices such as gaming consoles and global positioning system (GPS) receivers are also popular.
	IR transmission is a form of wireless transmission in which signals are sent via pulses of infrared light. IR is generally used for short-range transmission, because receivers need an unobstructed view of the sender to successfully receive the signal, though the signal can reflect off hard surfaces to reach the recipient. Typically, IR communication takes place in the near-infrared frequency range that is in the visible region of the spectrum. Therefore, in some instances, wireless IR communication is also referred to as wireless optical communication. IR uses electromagnetic waves with frequencies ranging from 300 GHz to 400 THz.

Infrared (IR)	Their wavelengths range from approximately 1 mm to 750 nm. IR waves are classified into sub-bands called far-infrared, mid-infrared, and near-infrared. The near-infrared frequencies are visible to the human eye as red or violet light, while the far-I frequencies are not visible to the human eye but are radiated in the form of heat. IR technology is used in several ways in the computing and telecommunication fields. The primary application is to provide network connectivity in wireless personal area networks. IR devices facilitate short-term wireless connections between two computers or between a computer and a wireless handheld device such as a mobile phone. An IR-powered network can also be used as an extension network for a local area network where installing cable may be difficult. Wireless devices such as wireless mice, keyboards, television remote controls, and game controllers also use *IR waves* for their operation.

Allocation of the RF Spectrum

The RF spectrum is classified based on the frequency range.

Frequency Range	***Name***
3 Hz–30 Hz	Extremely Low Frequency (ELF)
30 Hz–300 Hz	Super Low Frequency (SLF)
300 HZ–3KHz	Ultra Low Frequency (ULF)
3 KHz–30 KHz	Very Low Frequency (VLF)
30 KHz–300 KHz	Low Frequency (LF)
300 KHz–3000 KHz	Medium Frequency (MF)
3 MHz–30 MHz	High Frequency (HF)
30 MHz–300 MHz	Very High Frequency (VHF)
300 MHz–3000 MHz	Ultra High Frequency (UHF)
3 GHz–30 GHz	Super High Frequency (SHF)
30 GHZ–300 GHz	Extremely High Frequency (EHF)

ACTIVITY 1-2: Identifying Device Connections and Interfaces

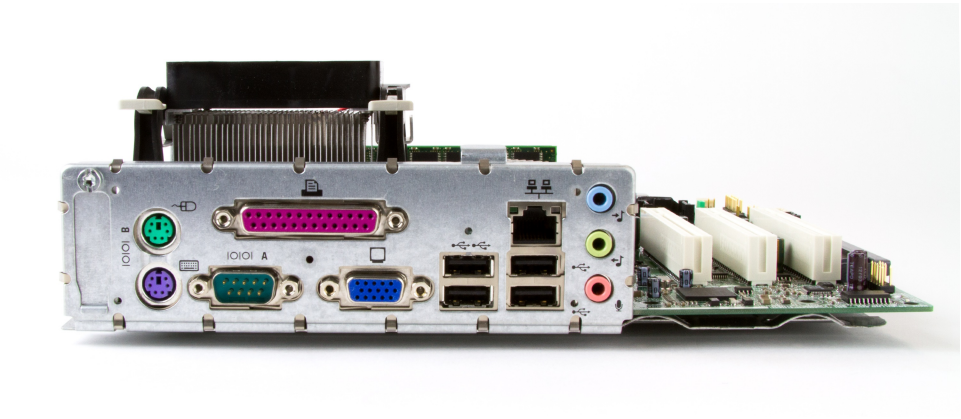
Scenario

In this activity, you will identify device connections and interfaces.

1. Your instructor might provide you with examples of device connections and interfaces and ask you or other participants to identify them.
2. **Examine the following graphic and identify the ports.**

   Identify the ports shown in the graphic. Use labels such as audio port, parallel port, PS/2 port, serial port, and USB port.

   A:



3. **Which connection type supports up to 127 peripherals for a single connection?**

   __ IEEE 1394
   __ SATA
   __ Parallel
   _x_ USB

4. **Which type of connection features small, thin data and power cables?**

   __ SCSI
   __ PATA
   _x_ SATA
   __ Parallel

5. **Which connection type transfers data eight or more bits at a time over eight or more wires?**

__ Serial connection
_x_ Parallel connection
__ USB connection
__ FireWire connection

6. **Which connection type connects a series of internal hard drives in a master/slave configuration?**

__ Parallel connection
__ USB connection
__ SCSI
_x_ PATA

7. **Which connection type is associated with the IEEE 1394 Standard?**

__ USB connection
_x_ FireWire connection
__ SCSI connection
__ Serial connection

Summary

In this lesson, you identified the components that make up most computers. The ability to identify the various parts of computers is essential foundational knowledge for every computer technician.

How many of the personal computer components described are familiar to you?

Which of the device connections discussed were familiar to you? Which were new?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 2: Operational Procedures

Lesson Time: 1 hour, 20 minutes

In the previous lessons, you gained fundamental knowledge about personal computer hardware components. In addition to that information, every PC technician also needs a working knowledge of tools, safety and environmental precautions, and when professional conduct is important in the workplace. In this lesson, you will identify the operational procedures that you should follow to ensure a safe working environment.

As an A+ technician, you will be asked to install, configure, maintain, and correct problems with a variety of PC components. To work with these components without damaging them or causing physical injury to yourself or others, there are several tools to use and operational procedures to follow in order to get the job done quickly, safely, and correctly.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Topic A:
  - Objectives 5.1, 5.2
- Topic B:
  - Objective 5.1
- Topic C:
  - Objectives 5.1, 5.2
- Topic D:
  - Objectives 5.3, 5.4

Topic A: Basic Maintenance Tools and Techniques

In this lesson, you will identify the operational procedures that can help ensure your success as an A+ certified professional. To begin, it's critical to select the right tool or technique for the job. In this topic, you will identify common hardware and software tools, maintenance techniques, and resources that are used by professional PC technicians.

When it comes to computer maintenance, having the right tool will save time, trouble, and money. Having a good collection of software and hardware tools at your disposal, a foundational knowledge of maintenance techniques, and access to documentation or resources when you need assistance is essential to help you perform your job tasks efficiently.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 5.1 Given a scenario, use appropriate safety procedures.
- Objective 5.2 Explain environmental impacts and the purpose of environmental controls.

Types of Hardware Toolkits

Because of the complexity of personal computers, there are several types of hardware toolkits that are commonly used in PC maintenance and repair.

Toolkit Name	***Description and Contents***
Basic	This toolkit should contain the tools necessary to remove and install computer components. Each tool should be demagnetized, and the tools should be stored in a case to protect and organize them. A basic toolkit should include: • Pen and/or pencil • Phillips screwdrivers (small and large, #0 and #1) • Flat-blade screwdrivers (small and large, 1/8-inch and 3/16-inch) • Flashlight • Container for screws • Nut driver Basic toolkits can also include: • Additional sizes of drivers and screwdrivers • Torx driver (size T8, T10, and T15) • Tweezers • Three-prong retriever • Ratchets • Allen wrenches • Cotton swabs • Batteries • Anti-static cleaning wipes • Anti-static wrist band

	• Compressed air canister • Mini vacuum • Pen knife • Clamp • Chip extractor • Chip inserter • Multimeter • Soldering iron and related supplies • Spare parts container • Circuit tester • Drive adapters (USB to IDE/SATA and SATA/PATA/IDE to USB)
Network	Specialized tools, in addition to those listed previously, are needed to make and install network cables. Kits containing these tools are available, but the prices vary widely depending on the quality of the tools. A network toolkit typically includes: • Cable crimper with dies for a variety of cable styles • Wire stripper for flat and coax cable • Precision wire cutters • Cable tester • Punchdown tool • Curved forceps • Multi-network Local Area Network (LAN) cable tester • Digital multimeter
	Usually circuit boards are replaced, not repaired. However, sometimes you can fix an obviously loose connection or replace a jack with a broken pin.

Circuit board	A circuit board toolkit typically includes: • 30-watt (W) ceramic soldering iron • Desoldering braid • Desoldering pump • Soldering iron stand with sponge • Solder • Miniature pliers and wire cutters • Heat sink

Software Diagnostic Tools

A *software diagnostic tool* or utility is a computer repair program that can analyze hardware and software components and test them for problems. Some software diagnostic tools can repair software problems and optimize settings. Most operating systems include several software diagnostic tools integrated into them. In addition, most computer stores have at least one aisle dedicated to utility software that has been developed by other software manufacturers.

Microsoft® Windows® 7 provides a few different software diagnostic tests that you can use to identify and repair computer hardware and software issues. For example, you can run the **Automatically fix file system errors** tool on any of your system drives by accessing the drive's **Properties,** selecting the **Tools** tab, and pressing **Check now.**

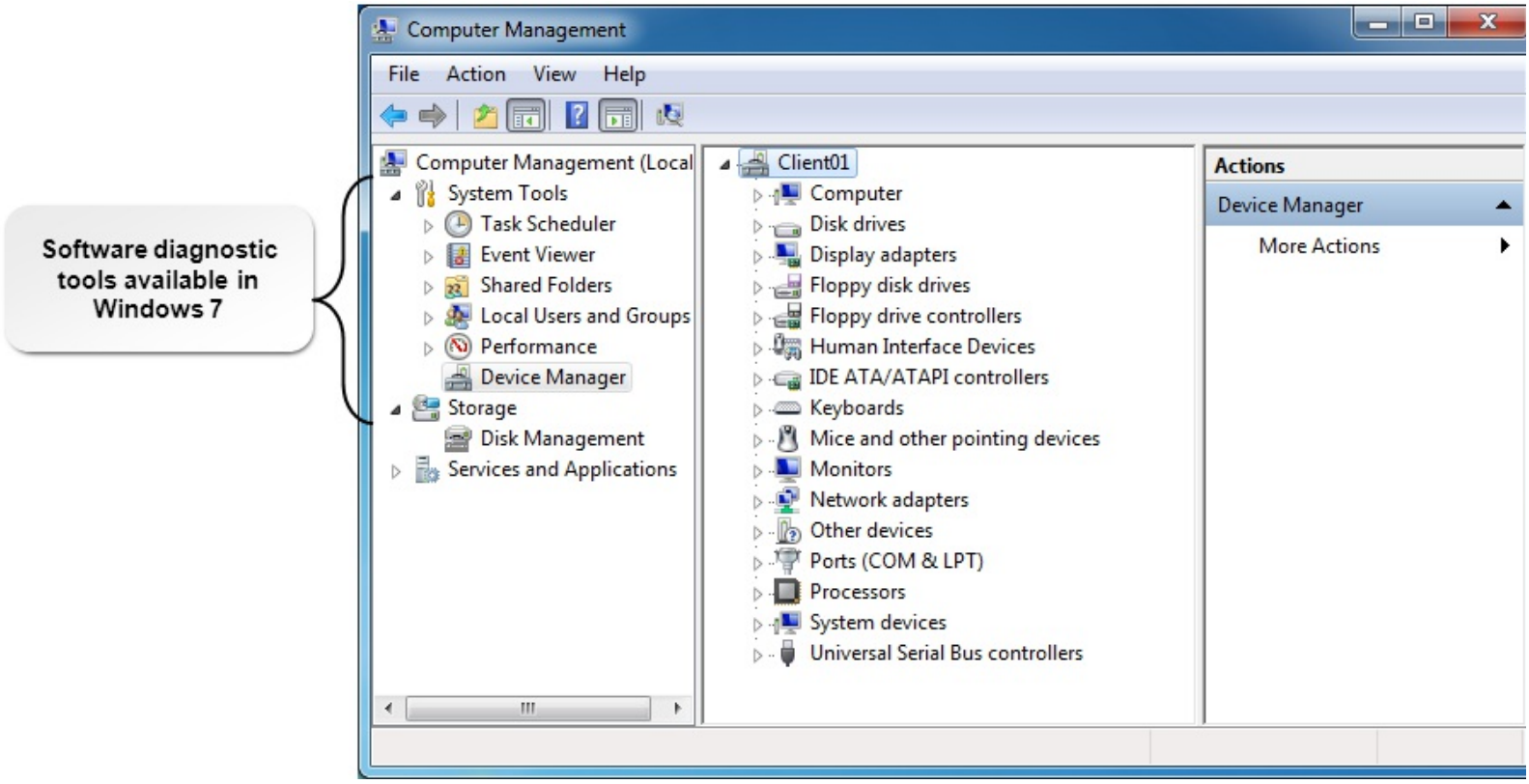


Figure: Software diagnostic tools.

Hard Drive Self-Tests

Most hard disk drive manufacturers provide a diagnostic tool that enables the drive to test itself when you start up a PC. Some of these hard drive self-tests are built into the firmware for the hard disk drive, while others are separate utilities that are available for download from the drive manufacturer's website. Make sure that you download the test utility that was designed to be used with your hard disk drive.

Software Diagnostic Tests

Software diagnostic tests are available from many different manufacturers, and they vary widely in their capabilities, but they can all assist you in detecting, repairing, and preventing hardware and software problems. The Windows operating systems also come with their own sets of diagnostic tools that can help you detect problems.

Examples of Software Diagnostic Tests

There are many applicable software diagnostic tests that you can use to troubleshoot computer problems.

Hardware Component	***Examples of Software Diagnostics Test***
Entire system	PC-Doctor Service Center, PC-Diag, Norton™ SystemWorks, QuickTech Pro, McAfee® System Mechanic, CheckIt Diagnostics, DirectX Diagnostic Tool, Windows **Device Manager,** Windows **Performance Monitor** There are many additional antivirus and anti-malware software solutions provided that detect and remove viruses, malware, and spyware.
Motherboard	Motherboard Diagnostic Toolkit, Power-On Self Test (POST), Basic Input/Output System (BIOS) setup
Central processing unit (CPU)	x86test, POST, BIOS setup
Memory	Memtest86+, DocMemory Diagnostics, POST, BIOS setup
Fan	SpeedFan, BIOS setup
Video adapter card	Video Card Stability Test, DirectX Diagnostic Tool, POST, BIOS setup
Network adapter card	3Com Dynamic Access Managed PC Boot Agent (MBA), Intel® PROset II Utility, DirectX Diagnostic Tool
Modem	Modem Doctor Diagnostics, DirectX Diagnostic Tool, Windows **Device Manager,** Windows **Performance Monitor**
Optical drive	CDRoller, Windows **Device Manager,** Windows **Performance Monitor**

Computer Component Maintenance Techniques

You can choose from several maintenance techniques to maintain PC components.

Maintenance Technique	***Description***
Use proper power devices.	Use a surge protector or *uninterruptible power supply (UPS)* to protect the computer from power surges, spikes, brownouts, and power failures.
Clean peripheral components.	Use to prevent problems with the computer's peripherals resulting from dust buildup.
Clean internal system components.	Use to prevent problems with internal computer components resulting from dust buildup.

Cleaning Compounds and Materials

LearnTO: For additional information, check out LearnTO **Clean a Desktop Computer** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Cleaning materials for computers range from standard household cleaning supplies to supplies specifically designed for computers and electronics.

Cleaning Supply	***Description***
Wipes and cloths	There are several types of wipes and cloths that you can use to clean displays, keyboards, and other equipment. • Monitor cleaning wipes are alcohol-based, lint-free, pre-moistened wipes for cleaning monitor screens. Use these only on cathode ray tube (CRT) or TV monitors and not on plastic-coated liquid crystal display LCD screens. • Keyboard cleaning wipes are pre-moistened wipes for cleaning keyboards. • You can use microfiber cloths to lightly remove dust and smudges from LCD displays. You can also use an LCD cleaning solution with the cloth to remove particles and smudges that are stuck to the screen. • If you choose not to use pre-moistened wipes, you can use rubbing alcohol applied to a lint-free cloth to wipe down screens and keyboards. You can also use this to clean other components. • A toner cloth is a special cloth that you stretch that picks up toner particles that are either in the printer or around the printer. Be careful if you are using it inside the printer so that the cloth does not get caught on any components and leave fibers behind.
	There are a variety of cleaning solutions that you can use to clean displays, keyboards, and other equipment. • You can use rubbing alcohol on cotton swabs or lint-free cloths to clean many components. • You can use mild household cleaner to keep the exterior of computer components clean. This helps prevent dirt and debris from getting inside the equipment. Never spray the cleaner directly on the equipment. Avoid using ammonia-based cleaners around laser printers; the ammonia may react chemically with the toner. • For older monitors, especially plastic monitors, read the device's manual to determine the cleaning method recommended by the manufacturer. While some recommend water or isopropyl alcohol (IPA), others claim it is acceptable to use

Cleaning solutions	volatile chemicals such as hexane or petroleum benzene, a soft detergent such as Palmolive and water, no suds, or nothing but a dry soft cloth. While some recommend a top-down motion, others subscribe to the circular method. • For flat screens such as LCDs, light emitting diodes (LEDs), and plasmas, you can use distilled water, or an equal ratio of water and vinegar on a microfiber or lint-free cloth. There are also specialized cleaners available for flat screens, but make sure to check the manufacturer's instructions before use. • In some cases, you can use standard household window cleaner on components if you spray it on a lint-free cloth first. You can use this to clean smudges from optical disks. Never use window cleaner on plastic monitor screens, and even on glass screens; this cleaner might strip off the anti-glare protection. The best option is a damp, clean, soft cloth with water or a cleaner specifically made for monitors (or one that states it is safe for use with monitors) and will not damage anti-glare finishes.
Cleaning tools	Several tools are optimal for cleaning computer components. • Tightly wound cotton swabs are useful in getting cleaning solution into tight places. They are also useful when used dry to get dust and debris out from between keys and around buttons or other tight areas. • Toothpicks come in handy in getting dirt out from around keys, buttons, and other tight spaces. They are also useful for removing the debris that builds up on the rollers inside of a mouse. • You can use a small paint brush to remove dust from between keys on a keyboard. If the brush has long bristles, they can reach under the keys where other cleaning objects would not be able to reach.
Compressed air canister	A canister with a nozzle that can be aimed at components to blow dust out. This is often used when removing dust from the interior of a computer or laptop. Be sure to blow the dust away from the power supply and drives. You can also use it to blow dust out of the power supply fan area, from keyboards, and from the ventilation holes on various components. Use caution when working with compressed air. Read the instructions on the can and follow them carefully. Tipping the can too much, which is easy to do when you are trying to maneuver the can into place, can cause the propellant to leave the can in liquid form and at sub-freezing temperatures. The freezing could easily damage components, particularly those that may still be hot from use. There is also the issue of the corrosiveness of the chemical damaging components later on. Also, some delicate components on the motherboard can be damaged (literally blown off the board) if compressed air is used too close to a component. If you use compressed air, take the equipment to a different location, preferably outside, so that the dust does not simply disperse into the air in the work area and settle back on

	the computer equipment or other devices.
Computer or electronics vacuum	A non-static vacuum that you can use on system components such as the power supply, fans, and in printers. (Regular vacuum cleaners can create static, which will damage computer equipment.) The vacuum should have a filter and bag fine enough to contain toner particles so that you can use it to clean up toner spills from laser printers or photocopiers. These vacuums can often be used to blow air as well as for suction, so they can replace the need for compressed air canisters for blowing dust out of machines. Sucking the dust up is usually better, though, since blowing the dust can cause it to get onto or into other components. Sucking it up into a vacuum cleaner bag gets it out of the system without the chance of it getting into something else.
Mask and gloves	A mask that fits over your mouth and nose should be worn when you are using a compressed air canister or working around toner spills. This will keep the particles out of your body. You should also wear latex gloves when cleaning up a toner spill.

Documentation and Resources

There are several types of documentation and resources that you might find helpful when you are dealing with common hardware and operating system problems. You can also share documentation and resources with users as a means of assisting and educating them.

Method	*Description*
User/installation manuals	User and installation manuals can provide you with basic guidance for installing, configuring, and troubleshooting hardware and software. By providing users with various user and installation manuals, users can fix minor issues and problems before requesting additional assistance from a technician. Examples include installing company-specific applications, installing network printers, and mapping drives.
Internet/web-based resources	Internet and web-based resources can provide a wealth of information on installing, configuring, and troubleshooting hardware and software. Many hardware and software manufacturers maintain knowledge bases and wikis to share information about both common and unusual issues that can arise with PC hardware and software. Internet and web-based materials can also provide users with quick reference materials for dealing with everyday issues on their own. Some organizations provide a web page or wiki with user-specific information and reference materials.
Training materials	Most major hardware and software manufacturers provide training materials on how to install and use their products. These materials can be helpful for both new and experienced technicians. You can provide training materials for various tasks that users may need to complete on their own, such as virus scans, computer maintenance tasks, and PC clean-up tasks. By providing training materials, you empower users to be proactive in maintaining their systems.

Compliance and Government Regulations

In the United States and many other nations, your employer is obligated to comply with government regulations that apply to its specific business. The most common regulations are those issued by the federal government, such as the Occupational Safety and Health Administration (OSHA), and state standards regarding employee safety. OSHA-compliant employers must provide:

- A workplace that is free from recognized hazards that could cause serious physical harm.
- Personal protective equipment designed to protect employees from certain hazards.
- Communication—in the form of labeling, Material Safety Data Sheets (MSDSs), and training about hazardous materials.

Your responsibility—to yourself, your employer, your coworkers, and your customers—is to be informed of potential hazards and to always use safe practices.

Protection of the environment is another area that is regulated by the federal and local governments in the United States and many other nations. Many municipalities have regulations that control the disposal of certain types of computer equipment. Your responsibility is to be aware of any environmental controls that are applicable to your workplace, and to be in compliance with those regulations.

ACTIVITY 2-1: Examining Basic Maintenance Tools and Techniques

Scenario

In this activity, you will examine the various tools and techniques used to maintain computer equipment and the workplace environment.

1. **You are asked to repair a motherboard in a customer's PC. Which set of tools would be best suited for the task?**

__ Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
_x_ 30-W ceramic solder iron, miniature pliers, wire cutters, and a soldering iron stand with sponge
__ Wire strippers, precision wire cutters, digital multimeter, and cable crimper with dies
__ Chip extractor, chip inserter, ratchet, and Allen wrench
__ Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs

2. **You are asked to correct a network cabling problem at a customer site. Which set of tools would be best suited for the task?**

__ Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
__ 30-W ceramic solder iron, miniature pliers, wire cutters, and a soldering iron stand with sponge
_x_ Wire strippers, precision wire cutters, digital cable tester, and cable crimper with dies
__ Chip extractor, chip inserter, ratchet, and Allen wrench
__ Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs

3. **You suspect that contaminants from the environment have prevented the fan on a PC from working optimally. Which set of tools would be best suited to fix the problem?**

__ Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
__ 30w ceramic solder iron, miniature pliers, wire cutters, and a soldering iron stand with sponge
__ Wire strippers, precision wire cutters, digital multimeter, and cable crimper with dies
__ Chip extractor, chip inserter, ratchet, and Allen wrench
_x_ Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs

4. **True or False? Windows includes software diagnostic tests that help you find and correct hardware problems.**

   _x_ True

   __ False

5. Examine the tools that are available to you in class. Discuss how and when they may be used to repair, fix, or maintain computer equipment.

Topic B: Electrical Safety

In the previous topic, you identified basic maintenance tools and techniques that you will use as a PC technician. In addition to these basic maintenance practices, you need to be aware of specific tools and techniques that are available to promote electrical safety. In this topic, you will identify the best practices for PC technicians to follow to promote electrical safety.

The most prevalent physical hazards that computer technicians face are electrical hazards. Electricity is necessary to run a computer, but it can also damage sensitive computer equipment, and in some cases, pose a danger to humans. Following established best practices for promoting electrical safety will protect not only the computer equipment that you work on, but also your personal safety and the safety of others.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 5.1 Given a scenario, use appropriate safety procedures.

Static Electricity

Static electricity is a build-up of a stationary electrical charge on an object. It is called "static" because the charge cannot escape the charged body until it comes in contact with another object. Static electricity is often caused by friction; rubbing one object against another causes a transfer of electrons between the two. Using friction to create a static charge is called *triboelectric generation.* The amount of static that can be built up in this manner depends on various factors, including the types of materials, their surface area and texture, and the ambient humidity. If you have ever shuffled your feet on a carpet and then gotten a small shock when you touched a doorknob or other metal object, you have used triboelectric generation.

Note: Static charges can be as small as the sparks that come off a dry blanket in the wintertime or as massive as a lightning strike, with its millions of volts.

ESD

Electrostatic discharge (ESD) occurs when a path is created that allows electrons to rush from a statically charged body to another with an unequal charge. The electricity is released with a spark. The charge follows the path of least resistance, so it can occur between an electrical ground, such as a doorknob or a computer chassis, and a charged body, such as a human hand. ESD can damage sensitive computer equipment.

Static Electricity and Voltage

Because air has very high resistance, a static electric discharge usually requires contact with the statically charged object. For a static discharge to arc through the air, it requires a very high voltage, and no other path to the ground with lower resistance. You can feel a static discharge starting at around 3,000 volts (V). The drier the air, the greater the resistance, which is why static shocks on dry winter days can fall within the range of 10,000 to 20,000 V. Keeping a room humidified is one way to reduce the risk of static electricity.

If 120 V from a household electrical outlet can kill you, why does a static spark of 20,000 V just startle you? Because, while the voltage might be high, the current is very low; very few total electrons are transferred in a static spark. All the energy of all the electrons in a spark added together cannot hurt you, even though it may surprise you. Each electron in a static discharge has extremely high energy, but the human body is just too big for the very small number of electrons involved in the spark to cause widespread damage. A few cells in your fingertip may be damaged, but they easily grow back.

ESD Prevention Techniques

Charges as low as 10 V can damage or destroy sensitive electronic circuits and components. This is why ESD is such an enemy of integrated circuits. Static charges can build up on both conductors and insulators, as well as in the human body. When you work with computer equipment, you must take steps to protect against ESD.

There are several prevention techniques that you can use to protect yourself and equipment when you are working with computer components.

Prevention Technique	***Description***
Eliminate activities and tasks.	By eliminating unnecessary activities that create static charges and by removing unnecessary materials that are known charge generators, you can protect against ESD-related damage and injuries.
Use self-grounding methods.	Use grounding conductive materials and self-grounding methods before touching electronic equipment. You can prevent ESD injuries by using ESD straps that can be attached to your ankle or wrist.
Use equipment grounding methods.	Grounding equipment made up of *dissipative material* can also be used to avoid a static shock. A dissipative material is a conductor, but with high resistance. It loses its electrical charge slowly, so when you touch it, the electron flow is spread over time and you do not feel a shock. Prevent ESD damage to equipment by: • Using anti-static vacuums for cleaning computer components (such as system units, power supplies, and fans). • Using ESD mats and materials such as electric grounded flooring, work benches, or surfaces. • Using anti-static bags to store computer components that are particularly sensitive to ESD, such as RAM and power supplies.
Maintain air quality.	You can maintain air quality and prevent a high-ESD work environment by: • Using an air ionizer, which releases negative ions into the air. They attract positively charged particles and form neutrally charged particles. • Humidifying the air to speed up the static discharge from components. When the air is extremely dry, more static is likely. A higher humidity is best for ESD prevention. A rate of 50 to 60 percent is comfortable for both computers and technicians.

Anti-static Bags

Anti-static bags that are used for shipping components actually conduct electricity, so keep them away from equipment that is powered on.

EMI

Electromagnetic interference (EMI) occurs when a magnetic field builds up around one electrical circuit and interferes with the signal being carried on an adjacent circuit, causing network communication interference issues. All current-carrying devices generate magnetic fields, and fluctuating magnetic fields generate electrical current in nearby wires. While ESD is the primary electrical danger to computer equipment, EMI also causes problems with microcomputer circuitry and data transmissions between computing devices.

Magnets

EMI-related issues can be a result of magnets being placed too close to computer systems. Magnets can be harmful to computer components, and components should not be placed in close proximity to any magnets or items that contain magnets. It's important that you inform users to keep magnets away from their computer equipment.

EMI Prevention Techniques

There are many different methods that you can use to prevent EMI damage to the internal circuitry of devices and systems.

Method	*Description*
Twisted-pair implementations	Twisted-pair cables are made with both sending and receiving conductors twisted together within the same cable. This method of manufacturing cable minimizes the chances of EMI interference because the conductors within the wire cancel each other out. For extra protection in multi-pair cables, such as Ethernet, each pair is twisted together at a different rate, and the multiple twisted pairs are then twisted together.
Cautious wiring techniques	The types of cables you use and how you place them can prevent certain devices and wires from interfering with each other. Fluorescent lights and alternating current (AC) electrical cables, for example, emit signals that are a source of EMI, so when you are running network cable in or along walls or ceilings, avoid running them near fluorescent fixtures, and try to cross electrical cables at right angles, rather than follow them. This minimizes the "cross-section" of interference from these sources. Electronic components themselves may generate or be susceptible to EMI; however, their leads serve as the antennae that radiate or receive such interference.
SMD technology implementation	Surface Mount Devices (SMDs) are electronic components that are designed to be soldered directly onto circuit boards without legs. This technology minimizes EMI transmissions to and from such devices.
Electromagnetic shielding	Shielding is used to prevent electromagnetic transfers from cables and devices by creating a conductive material protective barrier. For example, a shielded cable contains electromagnetic shielding within the cable that directly protects the inner core conductor from producing electromagnetic discharge.

Network Interference

Network interference is the disruption of normal data transmissions over a network. EMI can cause intermittent network issues and can be avoided by applying EMI prevention techniques such as shielding, wiring techniques, and using twisted pair cables to connect network components.

An ESD Toolkit

Some people who work on computer equipment never use a single piece of ESD safety equipment. They discharge themselves by touching an unpainted metal part of the computer case before touching any components. In other instances, a company policy might require that you use a properly equipped ESD-free work area. The minimum equipment in this case would be a grounded wrist ESD strap. Other ESD-protection equipment includes leg ESD straps, anti-static pads to cover the work surface, and grounded floor ESD mats to stand on. The mats contain a snap that you connect to the wrist or leg strap. Anti-static bags for storing components might also be included in an ESD toolkit. If the technician's clothing has the potential to produce static charges, an ESD smock, which covers from the waist up, can be helpful.

To ensure that the ESD equipment remains effective, you should test it frequently. A minor shock that you cannot feel can compromise ESD-sensitive equipment.

Figure: An ESD strap.

Electrical Hazards

Because computers are powered by electricity, there are some common potential electrical hazards that you should be aware of when you are servicing them.

Electrical Hazard	*Description*
Electric shock	If you touch a high-voltage source, and if you are either grounded or in contact with another electrical circuit, your body may complete an electrical circuit, permitting electrons to flow through you. Water is a better conductor than air or dry skin, so touching an electrical contact with wet hands reduces resistance and increases the current flow even more. Depending on the conditions, this may cause pain, burns, or even death.
Electrocution (fatal shock)	Electrocution results when the body is exposed to a lethal amount of electrical energy. For death to occur, the body must become part of an active electrical circuit with a current capable of overstimulating the nervous system or damaging internal organs. The extent of injuries received depends on the current's magnitude (measured in amperes), the pathway through the body, and the duration of flow. The resulting damage to the human body and the emergency medical treatment determine the outcome.
Burns	Contact with a source of electrical energy can cause external and internal burns. Exposure to higher voltages will normally result in burns at the sites where the electrical current entered and exited the body. High-voltage contact burns may display only small superficial injuries; however, the danger of these deep burns is destruction of internal tissues. Electricity can hurt you even if you are careful and avoid becoming part of an electrical ground circuit. The heat generated by an electric arc or electrical equipment can burn your skin or set your clothes on fire.
Collateral injuries	Collateral injuries occur when involuntary muscle contractions caused by the shock cause the body to fall or come in contact with sharp edges or electrically live parts. You instinctively pull your hand back from the doorknob when you get a static shock. Electricity flowing through your body can also cause your muscles to twitch uncontrollably. These motions can cause you to hurt yourself on objects around you.

Power Supplies and Electrical Hazards

Most of the internal circuitry in a computer is low voltage (12 V or less) and low current, so there is not much of a threat to your personal safety. However, there are exceptions to this, and these exceptions can be very dangerous. The main exceptions that you need to be aware of are power supplies.

- The computer's power supply outputs a relatively low voltage, but the high-voltage input can be

hazardous. PC technicians who have diagnosed a bad power supply should simply replace it, rather than open it to troubleshoot the internal components.

- The power supply in older CRT computer monitors increase the voltage, because CRT monitors contain circuits that require 35,000 V with a high current. In any power supply, the current is stored on capacitors that do not discharge, even when the component is turned off or unplugged. Even after months of inactivity, the capacitors may have enough stored electrical energy to kill you. Today, it is less likely than in the past that you will be working with CRT monitors, but if you find yourself in a situation where repair or maintenance is needed, leave the internal workings of the monitor to specialists who have the extra training and special equipment that are required to safely remove a monitor cover and make repairs. In most cases, it is less costly and faster to simply replace a defective monitor.

Laser Printer Electrical Safety

Laser printers contain high-voltage electronic components inside the case, and these components can be harmful if not handled properly. Components such as the rollers and wires can hold a charge, and you should avoid contact with them. Follow proper cleanup and safety guidelines to prevent electrical shock when you are working with laser printers.

ESD and Electrical Hazards

All of the precautions that you use to prevent ESD *increase* your danger when you work near high voltages. An anti-static wrist band is specifically designed to provide a low-resistance path for electricity to a ground. If there were ground problems or shorts, your body and your static protection equipment could provide a path from the problem device to ground—the circuit would be completed through your body, causing electrocution.

This is precisely why you must unplug devices that you are servicing. Even when devices are turned off, the power supplies in most devices continue to produce voltage if the device is plugged into an outlet. You and your anti-static devices could provide a better path to ground than the device's wiring, leading to your electrocution. If there is a chance of coming in contact with a high-voltage source, you are advised to insulate yourself from ground by wearing rubber-soled shoes or standing on a rubber mat, and avoiding contact with any other grounded mass.

Power Inverter Electrical Safety

A power inverter converts direct current (DC) voltage to AC voltage. For example, you can use a power inverter in a car to provide a normal wall-style outlet for a laptop. The power inverter unit has no user-serviceable parts within it, so after you determine that the inverter is a problem, there is no need for further diagnosis and troubleshooting; the unit must be replaced.

Electrical Safety Precautions

Working on a computer can be safe and enjoyable if you protect yourself from electrical hazards by using some common sense and by taking appropriate precautions.

Category	*Guidelines*
Personal safety	• Make sure that you disconnect the power before repairing computer equipment. • Do not attempt repair work when you are tired; you may make careless mistakes, and your primary diagnostic tool, deductive reasoning, will not be operating at full capacity. • Do not assume anything without checking it out for yourself. • Remove jewelry or other articles that could accidentally contact circuitry and conduct current. • Wear rubber-soled shoes to insulate yourself from ground.
Environment conditions	• Suspend work during an electrical storm. • Do not handle electrical equipment when your hands or feet are wet or when you are standing on a wet surface. Perform as many tests as possible with the power off.
Anti-static equipment	• Prevent static electricity from damaging components by standing on a totally insulated rubber mat to increase the resistance of the path to ground. In some cases, workstations are located in areas with grounded floors and workbenches, so static electricity has a low-resistance, non-destructive path to ground. • When removing circuit boards, place them on a dissipative ground mat or put them in an anti-static bag. • Use an anti-static wrist strap when you are handling static-sensitive components such as system boards, sound cards, and memory chips.
Disassembly safety	• After cleaning a keyboard, be completely sure it is dry before powering it up. • Label wires and connectors as you detach them, and make sure you that plug them back into the proper sockets in the proper order. • When you replace the computer's case, make sure that all of the wires are inside.

	The case may have sharp edges that can cut through exposed cables.
Power supply safety	• Power supplies have a high voltage in them any time the computer is plugged in, even if the computer power is turned off. Before you start working inside the computer case, disconnect the power cord and press the power button to dissipate any remaining power in the system circuitry. Leave the power off until you are done servicing the system unit. • Never stick anything into the power supply fan to get it to rotate. This approach does not work, and it is dangerous.
CRT monitor safety	• Do not take the case off a monitor. The risk to your life is not worth any repairs you might make. • Do not tap or bang on the monitor screen with your tools; an implosion will propel shards of glass in every direction. • To clean the monitor, turn it off and unplug it; do not wear an anti-static wrist strap. Use isopropyl alcohol, rather than a general-purpose cleaner; alcohol does not create a safety hazard if small amounts are dripped inside the case, as it will evaporate rapidly. Use an anti-static cleaner to clean the glass on the monitor. • Follow proper disposal guidelines if the CRT monitor cannot be repaired.
Electrical fire safety	Electrical fires in computer facilities are especially dangerous. The damage done to computers is extremely expensive, and the chemicals used in the machines may emit toxic substances. It is not practical to fight these fires with small extinguishers or to douse fires with water. Special gases should be used to extinguish fires in computer facilities. To prevent electrical fires: • Check the electrical wiring of computer systems and components regularly. • Implement a strategy to make sure any old, worn, or damaged cables, network appliances, and computer systems are checked and replaced regularly. • Verify that smoke detectors are installed to sense the presence of smoke. • Use heat sensors that are triggered either when a target temperature is reached or when there is a high rate of increase in temperature. • Use flame detectors with optical sensors to record incoming radiation at selected wavelengths. Commercial fire detection systems should be connected to a central reporting station

	where the location of the suspected fire is indicated. In some cases, the detection system or monitoring station is connected directly to a fire department.

ACTIVITY 2-2: Identifying Electrical Safety Issues

Scenario

In this activity, you will identify electrical safety issues.

1. **True or False? If you are using an anti-static ESD floor mat, you do not need any other ESD safety equipment.**

   __ True
   _x_ False

2. **Electrical injuries include electrocution, shock, and collateral injury. Would you be injured if you are not part of the electrical ground current?**

   A: Yes, you could receive a thermal burn from the head of an electric arc or electric equipment. Your clothes can catch on fire, or your skin can be burned.

3. **Which computer component presents the most danger from electrical shock?**

   __ System boards
   __ Hard drives
   _x_ Power supplies
   __ System unit

4. **Have you had any personal experience with any of the electrical hazards covered in this topic? What safety precautions could have prevented the incident?**

   A: Answers will vary depending on individual experiences. Common precautions include disconnecting a computer from the electrical outlet or power strip before servicing it, using anti-static equipment to protect computer components, and implementing smoke and flame detectors to alert you of electrical fires.

Topic C: Environmental Safety and Materials Handling

In the previous topic, you identified best practices for safely dealing with electricity. Electrical safety is just one factor that you need to consider to ensure a safe work area. In this topic, you will identify best practices for promoting environmental safety and proper materials handling.

In addition to electrical issues, there are other environmental issues that computer technicians must deal with on a regular basis. The health and safety of you and those around you should always be your highest priority. Recognizing potential environmental hazards and properly dealing with them in a safe manner is a critical responsibility for an A+ technician.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 5.1 Given a scenario, use appropriate safety procedures.
- Objective 5.2 Explain environmental impacts and the purpose of environmental controls.

Environmental Considerations and Controls

Certain environmental conditions can be extremely dangerous to you and those around you.

Consideration	*Description and Controls*
Ozone gas	Laser printers produce ozone gas, usually when the corona wire produces an electrical discharge during printing. Depending on the levels, ozone can be a mild-to-severe irritant. Regulatory agencies have established limits regarding the amount of ozone that employees can be exposed to. Be sure that your laser printers operate in a well-ventilated area. Some laser printers have a filter to control ozone emissions.
Temperature and humidity	Computer equipment and performance are both affected by temperatures and humidity levels. • Too much moisture can be problematic and cause physical damage to equipment. On the other hand, low humidity can contribute to more electrostatic charge into the air. High humidity levels can also have an effect on tapes and paper media. • Extreme temperatures can also be an issue. Low temperatures can cause condensation on computer system components that generate heat while turned on, while high temperatures can cause the components to overheat. Proper ventilation systems must be used to help prevent overheating of computer systems. Be aware of the humidity level and temperatures of the environment where devices will be installed and running to prevent these types of issues.
Dust and debris	Dust can be a more subtle hazard. The buildup of dust particles over time can cause problems with different types of equipment. Dust buildup causes resistance in moving parts, such as fans, drives, and printer motors. Dust buildup on circuit boards, heat sinks, and vents creates insulation that reduces heat dissipation. Dusting equipment often with compressed air and vacuums can prevent these types of issues. Make sure that printers and paper products are kept in a separate area from computer equipment to prevent paper dust from getting into the equipment.
Airborne particles	The conditions surrounding computer equipment can be an issue when there is a large number of airborne particles flowing in and around various devices. Contaminants can be either gaseous, such as ozone; particles, such as dust; or organic, which comes from industrial processing of fossil fuels, plastics, etc. All these contaminants can cause damage to computer equipment, such as corrosion and overheating. To protect your computing environment from airborne particles, you can: • Install computer equipment enclosures that will prevent contaminants from entering the devices. • Install air filters throughout the facility to catch excess particles as the air

	flows through the heating, ventilation, and air conditioning (HVAC) system.

Workplace Safety Issues

Various workplace situations can be a hazard to you and your coworkers.

Safety Issue	***Description***
Falling and tripping	Within your work area alone, a number of things can cause you to fall or trip. While working with computer equipment, you need to keep in mind the location of hardware, cables, and devices.
Equipment storage	CPUs and other hardware should not be stacked on top of one another. Make sure the equipment is secure, whether it is on the floor or on a desk or shelf.
Component handling and protection	Whenever you are handling computer equipment, you must follow the proper handling guidelines. Use an anti-static bag to store any computer component that can carry ESD. For example, when you are removing or replacing RAM, motherboards, or CPUs from inside a computer, immediately place the component in an anti-static bag until it is either replaced or disposed of.
Cable management	In office environments where there are many computers, there can also be many cables and power cords. If these cords and cables are lying on the floor, they could possibly cause a person to trip on them.
Lasers	Lasers are used in printers, CD drives, DVD drives, and Blu-ray drives and players. "Laser" is an acronym for Light Amplification by Stimulated Emission of Radiation. A laser produces an intense, directional beam of light by stimulating electronic or molecular transitions to lower energy levels. This powerful beam can cause damage to the human eye or skin. Lasers have many uses and, like other tools, are capable of causing injury if improperly used. The most likely injury is a thermal burn that will destroy retinal tissue in the eye. Because retinal tissue does not regenerate, the injury is permanent.
Repetitive strain injury (RSI)	Repetitive strain injuries involve damage to muscles, tendons, and nerves caused by overuse or misuse. Computer users suffer mostly from repetitive strain injuries to the hand, wrist, and arm. Unlike strains and sprains, which usually result from a single incident—called acute trauma—repetitive strain injuries develop slowly over time. The type of injury depends on whether the muscle, tendon, tendon sheath, or nerve tissue has been irritated or damaged. Any or all of the following symptoms may appear in any order and at any stage in the development of an injury of RSI: • Aching, tenderness, and swelling • Pain, crackling, and tingling • Numbness and loss of strength • Loss of joint movement and decreased coordination

Eye strain	Many computer tasks are done at a close working distance, requiring the eyes to maintain active focusing. This can cause stress and strain on the eyes and the muscles that control them. A very common health problem reported by users of computer monitors is eye strain—including the following symptoms: • Blurred vision • Difficulty focusing • Double vision • Tiredness • Headaches • Burning, sore, or itchy eyes Dry eyes can also be a concern for computer operators. The eye surface becomes dry because computer users tend to blink less and tears evaporate faster during monitor use. Symptoms associated with dry eyes are redness, burning, and excess tearing.
Radiation	Radiation is a broad term used to describe energy in the form of waves or particles. Electromagnetic radiation comes from both natural and manufactured sources, including CRT computer monitors. Circuits within the monitor are responsible for the horizontal and vertical movements of the electron beam. This movement occurs tens of thousands of times each second (Very Low Frequency, or VLF) for the horizontal scan, and 50 to 60 times each second (Extremely Low Frequency, or ELF) for the vertical scan. The VLF and ELF field intensities have been extensively evaluated in many different models of monitors for possible biological effects. CRT computer monitor users have expressed concerns about the possible health effects from the electromagnetic radiation that monitors produce. While the research continues, current scientific information does not identify a health risk from exposure to these electromagnetic fields. With CRT monitor use decreasing, concerns about radiation exposure have also declined.
Noise	Noise levels produced by computers and most printers are well below those that cause adverse health effects. The equipment has minor noise sources such as the hum of cooling fans and the clicking of keys. Excessive noise from a computer may indicate an internal malfunction. Certain industrial high-speed line printers may produce noise at a level which is uncomfortable for prolonged exposure; in these cases, sound-deadening covers are often used.
Hot components	Hot computer components within the system unit can be problematic. For example, any component carrying a high electrical voltage can get very hot and could cause burns. High-speed processors are also known heat generators; heat sinks and fans keep them cool enough to prevent a burnout, but they may still be uncomfortably hot to touch. You must exercise caution when working with any part of a computer or printer that may be hot to the touch, or that might be holding an electrical charge.

Food and drink	Eating and drinking around computer equipment can be problematic. Food particles and liquids can get inside and harm the inner mechanics of the hardware. Your employer may have policies in place that prohibit eating and drinking around computer equipment for these reasons.
Moving equipment	Lifting and moving computer equipment can be one of the more strenuous parts of your job. For example, when you need to work on a CPU, you may have to lift and relocate the machine to your work area. Always assess the situation first to determine if you can lift or move items safely.

Laser Safety Standards

To provide a basis for laser safety, standards are established for Maximum Permissible Exposure (MPE). Lasers and laser systems and devices are grouped into classes:

- Class 1 lasers do not emit harmful levels of radiation and are exempt from control measures.
- Class 2 lasers are capable of creating eye damage through chronic, continuous exposure; this class includes bar code readers.
- Class 3 lasers pose severe eye hazards when viewed through optical instruments (for example, microscopes) or with the naked eye.
- Class 4 lasers pose danger to eyes and skin, and are fire hazards.

Frequently, lasers are embedded in laser products or systems with a lower hazard rating. For example, laser printers, CD drives, and DVD drives are Class 1 laser products; however, they contain Class 3 or Class 4 lasers. When the printer or drive is used as intended, the controls for the device's class (Class 1) apply. When the system is opened—for example, for service—and the embedded laser beam is accessible, precautions must be based on the classification of the embedded laser (Class 3 or 4).

Environmental Safety Best Practices

To minimize the personal safety issues associated with computing environments, follow the recommended safety best practices and use the appropriate repair tools at all times.

Best Practice	***Safety Precautions***
Cords and cables	If cords and cables must traverse a floor area where people need to walk, it is recommended that cord protectors be used to shield the cords and cables from being damaged by pedestrian traffic, as well as to minimize the chance of someone tripping on the cords and cables. You can also use cable management techniques and tools to group and organize cables together to keep them out of the way and hidden from the general working space.
Lasers	Precautions include the following: • Never point a laser beam in someone's eyes. • Never look directly at a laser beam. • Never disable safety mechanisms when servicing a device with an embedded laser.
RSI	If an individual has even mild RSI symptoms, action should be taken. If symptoms are allowed to progress, a person with RSI can develop chronic symptoms. The key to RSI management is to remove an individual from the exposure that causes injury. A period of time away from the keyboard and mouse is followed by a gradual return to keying in an ergonomically correct work setting. Occasionally, a physician will prescribe a medication to help reduce symptomatic inflammation and pain. People with more severe forms of RSI may be referred by their medical provider to an occupational therapist who can do further evaluation and recommend a program of localized treatments, stretches, and exercises. Referral to an orthopedic hand specialist may be needed to determine treatment options. If the individual displays symptoms even at rest, splints may be recommended; while these are useful in the first stages of recovery, they are not the long-term solution. The best treatment for RSI, of course, is prevention through proper arrangement of computer workstations and reasonable project design.
Eye strain	A vision examination is recommended. A specific eyeglass prescription for computer use may help compensate for the strain involved in looking at a close and fixed point for periods of time. Artificial tears—used to supplement the eye's natural tear film and lubricate the dry surface—alleviate dry-eye symptoms for some computer users.
Noise	Impact printers and even the paper handling mechanisms on other industrial high-speed printers can be noisy and should be placed in rooms away from operators, where possible. Noise reduction hoods are recommended.

Lifting techniques	Before lifting anything: • Know your own strengths and weaknesses. You need to be aware of what your weight limitations are. • When you lift, bend at your knees and not at your waist. This will prevent strain on your back muscles and pressure on your spine. • Assess the equipment you are moving. If you feel that physically the equipment is too heavy or awkward for you to move alone, then get help from a coworker, or use a cart to relocate the equipment. If you use a cart, make sure the equipment is tightly secured during transport. • The equipment may be unstable for lifting. You may need to take special precautions and may require help moving it to a cart. • Equipment should never be stacked too high while moving to avoid hardware falling and breaking on the floor. This can cause damage to other devices or to you. • Plan ahead. While moving equipment from one area to another, be aware of narrow doorways or columns that you will encounter on the way. Also, make sure to prep the space before delivering the equipment so that you are not trying to reconfigure the space with all the equipment in the way.

General Power Issues

Power issues can cause a number of problems for computer equipment and the working environment. Computer equipment, printers, network devices, and other resources require power, so any disruption in electricity will present a number of issues. There are several power problems that can occur.

Power Problem	***Description***
Blackout	A *blackout* involves a complete loss of power.
Brownout	A *brownout* is a temporary power reduction that is often used by electrical power companies to deal with high power demands. It is called a brownout because the lights dim during the event.
Sag	A *sag* is a momentary low-voltage power failure.
Spike	A *spike* is a short-term, high-voltage power malfunction.
Surge	A *surge* is a long-term, high-voltage power malfunction.
In-rush	An *in-rush* power problem is a surge or spike that is caused when a device that uses a large amount of current is started.

Power Protection Systems

There are several protection systems that can restore power to some operational capacity, decrease failures, or monitor power sources.

Power Protection System	***Description***
UPS or battery backup	An *uninterruptible power supply (UPS)*, also referred to as a *battery backup*, is a device that continues to provide power to connected circuits when the main source of power becomes unavailable. Depending on the design, UPSs can be battery operated, AC powered, or both. They are meant for temporary use and are intended to support computer systems until they can be powered off normally. Power is likely to be interrupted when the batteries or other power sources are discharged.
Generators	A *generator* creates its own electricity through the use of motors. Generators provide long-term power and are often started while a UPS system supports equipment through the initial power loss. Generators can fail when motor fuel runs out or when a mechanical failure occurs.
Surge suppressor	A *surge suppressor* is a device that provides power protection circuits that can reduce or eliminate the impact of surges and spikes.

UPS Types

Depending on the needs of an organization, different types of UPSs might be used. Common types include:

- A standby UPS, which is primarily AC-powered, until the power source fails. When the power source fails, it switches to the backup power source or battery. This UPS is used most often with personal computers.
- A line interactive UPS is commonly used in smaller business settings to provide power through a constant AC connection. When the AC power fails, the inverter switches to battery power. This UPS is unique in that while the AC power is available, it is used to also charge the battery.

Liquid Hazards

There are many different professional situations when you may come in contact with a hazardous liquid. Some such compounds are used to clean or condition equipment, including the computer's case, adapter card contacts and connections, and glass surfaces. They may present safety or environmental problems. Make sure you read the labels and follow the instructions carefully when you are disposing of hazardous materials.

Chemical Hazards

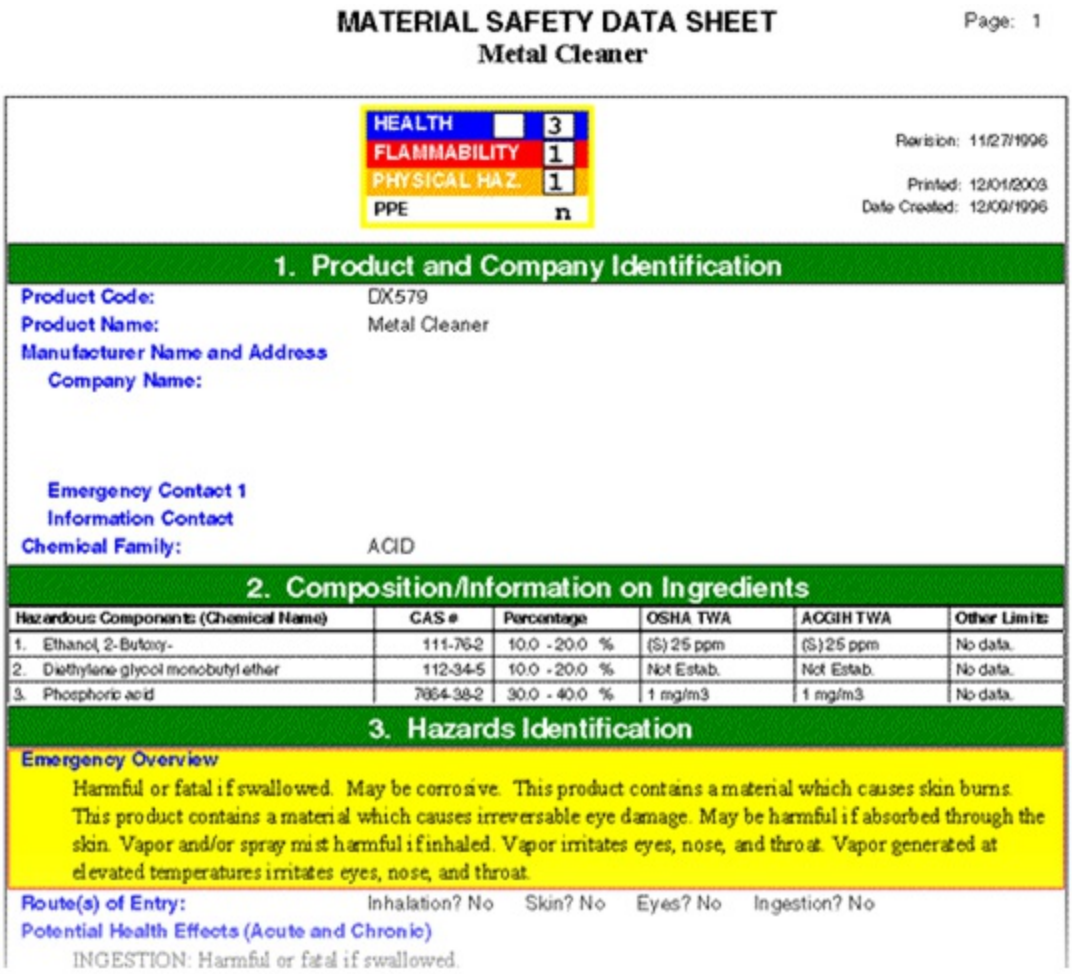
Working with personal computers can cause you to come in contact with some chemical hazards.

Chemical Hazard	*Description*
Laser printer toner	Made of fine particles of iron and plastic, toner presents its own set of problems due to its reactions with heat. If you spill toner, do not clean it up with a regular vacuum; the particles will get into the motor and melt. Do not use warm water to wash toner off your hands or arms; the toner could fuse to your skin. Instead, brush off as much as you can with a dry paper towel, rinse with cold water, and then wash with cold water and soap. In addition, do not use ammonia-based cleaners on or around laser printers, as the ammonia may react chemically with the toner.
Batteries	Batteries maintain the data in complementary metal oxide semiconductor (CMOS) chips and supply power to remote controls, portable computers, and other devices. These batteries may contain mercury, cadmium, and lithium, as well as other dangerous chemicals.
Capacitors	Capacitors store electricity by using two or more conducting plates separated by an insulator. There are capacitors in various personal computer components, including microprocessors. The electrolytes in capacitors are very caustic; treat them as you would any hazardous chemical. Thoroughly wash your hands after handling ruptured capacitors.

Caution: The capacitors in power supplies and monitors do not discharge when they are turned off or unplugged, and contain enough charge to kill you. Do not open or attempt to service internal components of power supplies or monitors.

MSDS Documentation

A *Material Safety Data Sheet (MSDS)* is a technical bulletin that is designed to give users and emergency personnel information about the proper procedures for the storage and handling of a hazardous substance. This applies to any situation in which an employee is exposed to a chemical under normal use conditions or in the event of an emergency. The manufacturers supply MSDSs with the first shipment to a new customer and with any shipment after the MSDS is updated with significant and new information about safety hazards. You can get MSDSs online; the Internet has a wide range of free resources. OSHA regulations govern the use of MSDSs and the information an MSDS must contain.



MATERIAL SAFETY DATA SHEET
Metal Cleaner

Page: 1

HEALTH 3
FLAMMABILITY 1
PHYSICAL HAZ. 1
PPE n

Revision: 11/27/1996
Printed: 12/01/2003
Date Created: 12/09/1996

1. Product and Company Identification

Product Code: DX579
Product Name: Metal Cleaner
Manufacturer Name and Address
Company Name:

Emergency Contact 1
Information Contact
Chemical Family: ACID

2. Composition/Information on Ingredients

Hazardous Components (Chemical Name)	CAS #	Percentage	OSHA TWA	ACGIH TWA	Other Limits
1. Ethanol, 2-Butoxy-	111-76-2	10.0 - 20.0 %	(S) 25 ppm	(S) 25 ppm	No data.
2. Diethylene glycol monobutyl ether	112-34-5	10.0 - 20.0 %	Not Estab.	Not Estab.	No data.
3. Phosphoric acid	7664-38-2	30.0 - 40.0 %	1 mg/m3	1 mg/m3	No data.

3. Hazards Identification

Emergency Overview
Harmful or fatal if swallowed. May be corrosive. This product contains a material which causes skin burns. This product contains a material which causes irreversable eye damage. May be harmful if absorbed through the skin. Vapor and/or spray mist harmful if inhaled. Vapor irritates eyes, nose, and throat. Vapor generated at elevated temperatures irritates eyes, nose, and throat.

Route(s) of Entry: Inhalation? No Skin? No Eyes? No Ingestion? No
Potential Health Effects (Acute and Chronic)
INGESTION: Harmful or fatal if swallowed.

Figure: An MSDS.

Required Information in an MSDS

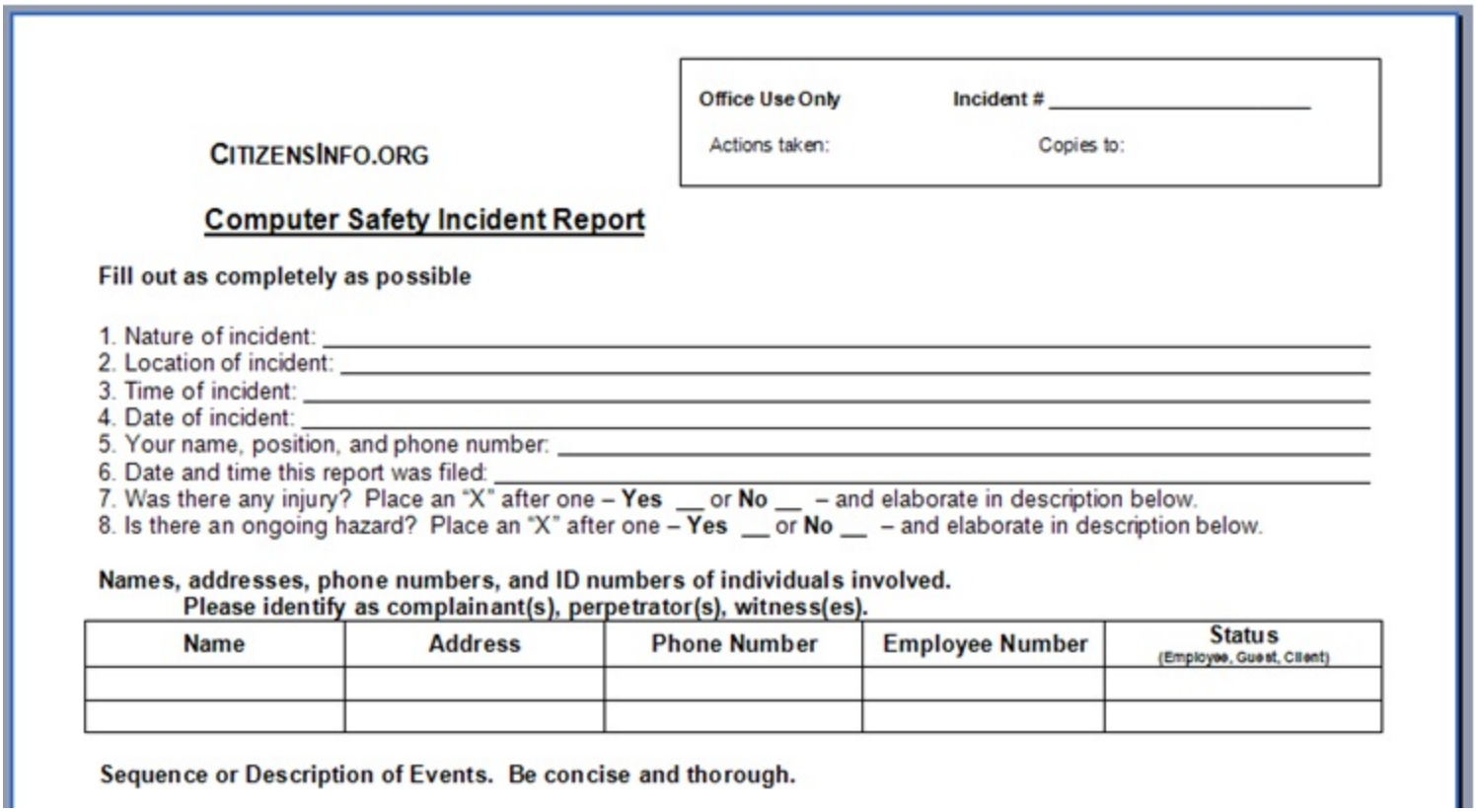
Every MSDS is required to include information about the following items:

- Physical data
- Toxicity

- Health effects
- First aid
- Reactivity
- Storage
- Safe-handling and use precautions
- Disposal
- Protective equipment
- Spill/leak procedures

Incident Reports

An *incident report* is a record of any instance where a person is injured or computer equipment is damaged due to environmental issues. The report is also used for accidents involving hazardous materials, such as chemical spills, that could have an impact on the environment. Any time an accident occurs at a work site, you should submit an incident report. Reporting these occurrences is often part of company policy and can help provide protection against liability.



Office Use Only Incident # _____

Actions taken: Copies to:

CITIZENSINFO.ORG

Computer Safety Incident Report

Fill out as completely as possible

1. Nature of incident: _____
2. Location of incident: _____
3. Time of incident: _____
4. Date of incident: _____
5. Your name, position, and phone number: _____
6. Date and time this report was filed: _____
7. Was there any injury? Place an "X" after one – **Yes** __ or **No** __ – and elaborate in description below.
8. Is there an ongoing hazard? Place an "X" after one – **Yes** __ or **No** __ – and elaborate in description below.

Names, addresses, phone numbers, and ID numbers of individuals involved.
Please identify as complainant(s), perpetrator(s), witness(es).

Name	Address	Phone Number	Employee Number	Status (Employee, Guest, Client)

Sequence or Description of Events. Be concise and thorough.

Figure: Sample incident report.

Hazardous Material Disposal Procedures

Proper disposal of hazardous materials is an essential part of maintaining a safe work environment.

Hazardous Material	***Disposal Recommendations***
Liquid cleaning materials and empty containers	Follow your company's guidelines for disposing of liquid cleaning materials and their containers. Each municipality has its own disposal regulations that you must learn and follow. You can find out about these regulations by contacting your local government's environmental office or department for trash disposal and recycling.
Toner	Empty toner cartridges should not be discarded in the trash because of the damage that the residual chemicals can do to the environment. Used toner cartridges should be refilled or returned to the manufacturer for recycling and/or disposal. Follow your company's guidelines for disposal procedures.
Display devices	The CRTs in older computer monitors contain lead, which is considered a hazardous material. Follow your company's guidelines for disposing of display devices. Many municipalities have regulations for disposal and recycling of old monitors and television sets; contact your local government's environmental office or department for trash disposal and recycling to determine if there are specific rules you need to follow.
Ozone filter	Follow the manufacturer's recommendations for replacement and disposal of a laser printer's ozone filter.
Batteries	Used batteries should not be discarded in the trash; they should be recycled or disposed of following your company's guidelines.

ACTIVITY 2-3: Identifying Environmental Safety Issues

Scenario

In this activity, you will identify the best practices for promoting environmental safety and proper handling of materials.

1. **You are on a service call, and you accidentally spill some liquid cleaner on the user's work surface. What actions should you take?**

   _x_ Refer to the MSDS for procedures to follow when the material is spilled.
   __ Wipe it up with a paper towel and dispose of the paper towel in the user's trash container.
   _x_ Report the incident.

2. **Ozone is classified as an environmental hazard. Which device produces ozone gas?**

   _x_ Laser printer
   __ CPU
   __ Laptop
   __ Power supply

3. **What item reacts with heat and ammonia-based cleaners to present a workplace hazard?**

   __ Capacitor
   __ Laser
   _x_ Toner
   __ Battery

Topic D: Professionalism and Communication

So far in this lesson, you have identified best practices for working directly with computer equipment. On almost every service call, you will also need to interact with users who are experiencing problems. In this topic, you will identify best practices for PC technicians to use to communicate appropriately with clients and colleagues and to conduct business in a professional manner.

You are a representative of your profession, as well as your company. Working with customers is a fundamental job duty for every A+ technician. How you conduct yourself will have a direct and significant impact on the satisfaction of your customers, and your level of professionalism and communication skills can directly affect whether or not you will do business with them again in the future.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 5.3 Given a scenario, demonstrate proper communication and professionalism.
- Objective 5.4. Explain the fundamentals of dealing with prohibited content/activity.

Communication Skills

Using the proper communication skills when dealing with clients and colleagues creates a professional environment that is conducive to solving the problem at hand.

Communication Skill	*Description*
Use proper language	• Use clear, concise, and direct statements. This will help you get to the crux of the matter more quickly, and it will help the user understand what you are saying. • Avoid using jargon, abbreviations, acronyms, and slang. Many users will not have the same level of technical knowledge as you and your colleagues, and using terminology that is beyond their level of knowledge can confuse or upset them. • Use timing to set the pace of a conversation. A pause may be more valuable than an immediate answer, as it allows you time to formulate your response. If a situation escalates and your customer becomes agitated, you may ask him or her to slow down so that you can get all the information. When a customer is having difficulty ending a call to the help desk, you may gently step up the pace to indicate your need to move on.
	• Be aware of the non-verbal clues you use, whether you are talking or listening. Body language communicates more than actual words. Studies show that up to 70 percent of a message is conveyed through actions. Even when you are talking on the phone, non-verbal characteristics—such as tone of voice—will add meaning to your message and help you interpret your customer's concerns. • Use the proper level of eye contact. You and your customer will make, maintain, and break eye contact as you talk with each other. When attention is directed to the problem at hand, eye contact may be minimal. Avoid staring directly at your customer—a form of invading personal space—or letting your gaze wander, which indicates disinterest, or even worse, inappropriate interest. • Use gestures and facial expressions to reinforce your spoken message. Broad, friendly gestures indicate being open to the conversation, while sharp or jabbing gestures usually mean anger. The variety, intensity, and meaning of facial expressions are almost endless. You and your customer read each other's faces to gain insight into the spoken words. Your expression must match the content of your words; if there is a mismatch, your customer will

Non-verbal communication	believe the message in your face, rather than what you say. • Use non-verbal encouragement to gather information. Encourage your customer to continue with "Mm-hmm" and a slight nod of your head. You convey that you are listening and want to know more. • Be aware of physical positioning and posture. Respect your customer's personal space. Depending on the circumstances, you may be from 1.5 to 4 feet away from your customer. If the customer backs up, you are too close. You may be working in close quarters; ask permission before you move into your customer's personal space—for example, sitting in the office chair. Messages are conveyed by body position. Slouching indicates: "I am bored with this conversation." Holding one's arms across the chest says: "I am closed off to what you are saying." Watch your body's signals, as well as those of your customer. • Be aware of the effect of tone of voice, which can indicate many internal moods: excitement, boredom, sarcasm, fear, or uncertainty. A rise in your voice at the end of a sentence makes it sound like a question, implying lack of assurance instead of competence. Listen to your customer's tone. Volume —loudness or softness—colors the spoken message. If your customer's agitation escalates, try lowering your volume to re-establish a sense of calm. • Use the appropriate level of physical contact. A firm handshake is appreciated and may be expected in some business dealings. Other forms of touching are generally unnecessary, inappropriate, and risky.
Listening skills	• Listen and do not interrupt the customer. If your attention drifts or you interrupt, you run the risk of missing some important information that can help you solve the problem. • Allow the user to complete statements—avoid interrupting. This will convey the message that you respect the user and want to hear what he or she is saying. • Employ passive listening techniques. Your message is: "I am listening. Tell me more." You are alert, attentive, and accepting, but do not participate actively in the conversation. Your silence may help your customer to collect his or her thoughts, especially if he or she is upset or angry. Listen for factual data and be alert for feelings and attitudes, which are conveyed non-verbally. It may be difficult to keep from jumping in with a question or a "Yes, but..." Resist the temptation by writing down your thoughts to refer to later. • Employ active listening techniques. When your customer is describing the

	problem, listen actively to elicit as much information as you can. Clarify user statements by asking pertinent questions.

Active Listening

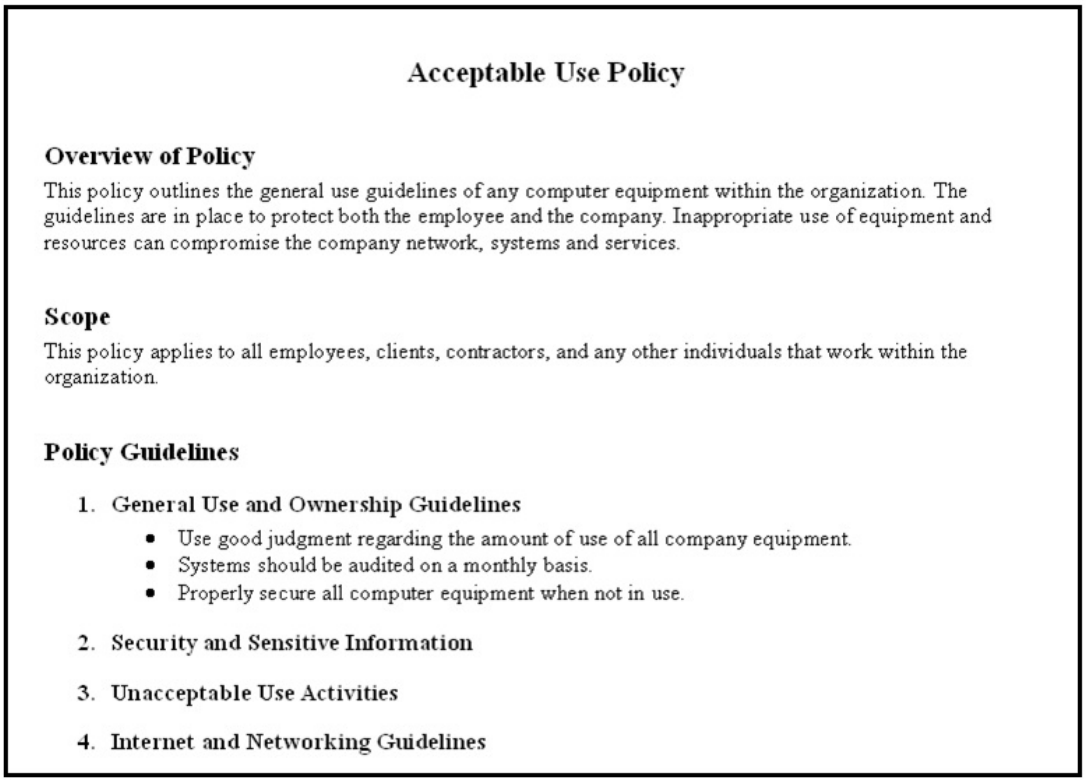
Active listening techniques can enhance your communications skills. These techniques may feel awkward at first, so you might want to try them out in a situation outside your job. With practice, you will use active listening skills more easily and creatively.

Action	*Description*
Questioning	Ask questions to gain information, clarify what you have heard, and direct the conversation. Open-ended questions can elicit a lot of information. Close-ended questions limit the amount of information by giving a choice of answers. Yes/no questions further limit the information exchange and can be used when you need to get closer to a conclusion. Examples of each of these question styles are: • Open-ended: "What happened after you pressed Ctrl+Alt+Delete?" • Close-ended: "What kind of a printer do you have, laser or inkjet?" • Yes/no: "Are you on a network?" What if the answer to your open-ended question is "I do not know" or "I am not sure"? Go down the list—using close-ended and then yes/no—until you reach the customer's level of expertise. Examples of less helpful question styles: • Confusing multiple questions: "What did you do next? Did you try...? What happened?" • Accusations: "What did you do that for?"
Empathizing	Let your customer know that you perceive and support what they are feeling. Try to be specific in naming the emotion and link it to the customer, using "you," not "I." Examples of helpful empathetic responses include: • "This delay is frustrating for you." • "You are afraid you will lose business while your computer is down." • "You must be worried about the cost." Examples of less helpful empathetic responses include:

	• "I know how you are feeling." • "I can identify..."
Paraphrasing	Restate what the customer says in your own words to make sure that you interpreted correctly, to bring order to the customer's thoughts, and to relay that their message is important. Use statements, not questions, and do not add or change anything. Examples of starters for paraphrasing include: • "You are saying that..." • "It sounds like..." • "I am hearing you say..."
Summarizing	Outline the main points of your conversation to summarize what has been said. You can begin by summarizing your understanding of the problem and then checking for clarification. During the conversation, you can re-establish the focus by listing the important facts. Bring closure by summing up the work performed. If a follow-up plan is needed, restate the responsibilities and timeline. Helpful starters for summarizing include: • "Let's see what we have so far." • "Why don't we back up a minute and go through that again?" • "Let's go over our plan."

Organizational Policies and Procedures for Appropriate Use

Organizational policies are documents that convey the corporate guidelines and philosophy to employees. Policies can be either high-level corporate documents distributed to the entire organization, or lower-level operational documents that affect only certain departments, divisions, individuals, or roles in an organization. For example, most organizations will have an *acceptable use policy (AUP)* that includes practices and guidelines that management expects all employees to follow when they are using and accessing company-owned computer equipment and information-related resources.



Acceptable Use Policy

Overview of Policy

This policy outlines the general use guidelines of any computer equipment within the organization. The guidelines are in place to protect both the employee and the company. Inappropriate use of equipment and resources can compromise the company network, systems and services.

Scope

This policy applies to all employees, clients, contractors, and any other individuals that work within the organization.

Policy Guidelines

1. General Use and Ownership Guidelines
   - Use good judgment regarding the amount of use of all company equipment.
   - Systems should be audited on a monthly basis.
   - Properly secure all computer equipment when not in use.
2. Security and Sensitive Information
3. Unacceptable Use Activities
4. Internet and Networking Guidelines

Figure: An AUP.

Professional Conduct

Acting in a professional manner when dealing with colleagues and clients provides a work environment where problems can be solved efficiently.

Facet	*Description*
Appearance	Exhibit a professional appearance. Your work environment may be in a repair shop, at a help desk, or on-site at the customer's business. Whatever the situation, you will want to present a neat, clean, business-like appearance. On-site work may take you into many settings, from muffler repair shops to executive offices. You may be asked to remove your shoes or put on a hard hat. Be aware of the corporate culture and respond accordingly.
Respect	Be respectful of the customer and the environment in which you are working. • Maintain a positive attitude when talking with users. Avoiding arguing or getting defensive with users will make it easier for you to solve the problem to the user's satisfaction. • Be culturally sensitive. Always be conscious of who you are working with, and how your actions can be conveyed. • Do not minimize the customer's problem. What seems simple to you could be a mission-critical problem to the user. • Never insult a customer or call the customer names. No matter how frustrating a service call might become, rudeness is never the answer. • When you are dealing with customers, avoid distractions and interruptions. Repeatedly answering a mobile phone, talking to coworkers, or attending to any other personal distractions while you are supposed to be working on a problem sends the message that the user's problem is unimportant to you. • Ask open-ended questions and try and narrow the scope of the problem. Restate the issue or question to verify understanding. This will show the customer that you are listening and care about resolving the issues at hand. • Be sure to keep your work area at the customer site neat. Do not pile materials on your customer's books and files. Clean up after yourself. When you are on-site, ask where to dispose of materials; find out where the recycling bin is for printer test-run paper. • Be on time. Tardiness can give the customer a negative impression of you. If you are going to be late, always call and communicate with the customer. • Be respectful of the property at the customer site. Always ask permission before entering an office or workspace, using the telephone, sitting down at a computer,

	or adjusting the workspace.
Accountability	Be accountable. Do not misrepresent your credentials, competence, or training. Take responsibility for your actions, and admit your mistakes. In questions of conflict of interest between your company and the customer, refer to your supervisor or follow your company's procedures. Be aware of your company's policy for accepting gifts or samples, and for socializing with customers.
Confidentiality	Treat any information located on a desktop, a computer, or a printer that pertains to your customer's business as confidential. Know your company's policies concerning confidential information—and follow them. Many fields—including medicine, social work, and special education—are regulated by federal and state laws concerning the confidentiality of their customers, consumers, or clients. All companies have personal information about their employees. Many corporations have sensitive information about the development of their products or services.
Honesty	Be forthright with your customers about what is occurring and the actions you will take. Clients have a right to understand the process you are following and how it will affect them. Discourage software pirating. Software copyright infringement, or pirating, relates to the legal issues surrounding the distribution and use of software. The Federal Copyright Act of 1976 protects the rights of the holder of a copyright. Typically, a backup copy of software is allowed and a site license allows for the use of multiple copies at one facility. You are responsible for upholding the law by complying with the license agreements that both your company and your customer hold. Learn your company's policies and adhere to them. Pirating carries penalties and risks, including fines, imprisonment, corrupted files, virus-infected disks, discontinued technical support, and upgrade unavailability.
Prioritizing	Set priorities. You will often need to set priorities and make judgment calls. You will recommend whether your customer should repair or replace equipment. You will rank the urgency of your customers' needs. Base your decisions on common courtesy, fundamental fairness, and keeping promises. Be familiar with your company's policies and follow them.
Expectations	You should set and meet customer expectations up front. Set a timeline and a communication plan that both you and the customer agree to at the start of the business relationship. Always communicate repair and replacement options, and provide the proper documentation needed for the services provided. Always follow up and get customer feedback on the work completed. This information allows you to improve customer satisfaction.
Ethics	Practice ethical conduct. You have an obligation to take responsibility for ethical conduct within your delivery of service. Ethical issues are complex and ever-changing in the computer industry. An unethical practice may become so routine that it is falsely assumed to be acceptable behavior. Learn your company's policies and adhere to them.

Prohibited Content

As an A+ technician, you may come across situations when you may encounter prohibited activities, such as viewing pornography on work-issued devices by users either within your organization or by a customer. There are different levels of prohibited content, which can be described as distasteful, inappropriate, or illegal. Every organization will have different guidelines and restrictions based on the type of content. For example, some organizations will discourage access to social networking sites, or websites that contain questionable words or phrases, but will not explicitly forbid it. On the other hand, restrictions on content or data that can be categorized as inappropriate or illegal, such as pornography, will be enforced heavily, and accessing such content will have immediate consequences. In each of these cases, it is your responsibility to follow organizational procedure to report the incident. When reporting potentially illegal activities, you must follow the organization's policy on reporting, collecting, and documenting the specifics of the situation and what evidence was found.

Best Practices Related to Prohibited Content or Activity

The process of identifying and reporting prohibited content or activity can be complicated, especially when an organization does not have sufficient policies and documented guidelines. There are some fundamental methods that can be applied to help properly report, document, and resolve issues.

Phase	*Description*
First response	*First response* refers to the immediate actions that follow an incident, as well as the individual or individuals who perform these actions. There are a few actions that take place during the first response to an incident: • Identifying the data and/or hardware. • Reporting the details of the discovery and evidence through the proper channels. This will vary depending on the specific organization's policies and reporting instructions. • Preserving the data and/or device as evidence. This can sometimes be also be called computer forensics.
Chain of custody	The *chain of custody* is the record of tracking evidence from collection through presentation in court. The evidence can be hardware components, electronic data, or telephone systems. The chain of evidence reinforces the integrity and proper custody of evidence from collection, to analysis, to storage, and presentation in a court of law. Every person in the chain who handles evidence must log and document the process, methods, and tools they used.
Documentation	In the process of identifying and reporting incidents with prohibited content, you should follow the organization's documented procedures to ensure that you are carrying out the correct response tasks and guidelines. You must also be aware of any changes made to the documentation so that you are always following the right procedures in handling incidents, managing evidence, and reporting findings to the appropriate individuals.

Computer Removal

When computer crimes are reported, one of the first response activities is removing computers from the crime location. They are tagged with a chain of custody record to begin the process of making the evidence secure for future presentation in court.

Anti-Spyware Software

Anti-spyware software is specifically designed to protect systems against spyware attacks. Some antivirus software packages include protection against adware and spyware, but in most cases, it is necessary to maintain anti-spyware protection in addition to antivirus protection. Some examples of anti-spyware include Webroot's Spy Sweeper and STOPzilla Anti-Spyware. This can help prevent

users from accidentally clicking on advertisements that would take them to unauthorized sites or installing malicious software through a pop-up advertisement.

Computer Forensics

Computer forensics is the practice of collecting and analyzing data from storage devices, computer systems, networks, and wireless communications and presenting this information as a form of evidence in a court of law. Primarily, forensics deals with the recovery and investigation of potential evidence. Computer forensics is a fairly new field, so there is little standardization or consistency in practicing it across organizations and courts. Basically, computer forensics is a blend of the elements of law with computer science in analyzing evidence in a way that is permissible in the court of law.

Basic Forensic Response Procedures for IT

Forensic response procedures for IT help security professionals collect data evidence in a form that is admissible in a court of law.

Forensic Response Procedure	***Description***
Capture system image	One of the most important steps in computer forensic evidence procedures is to capture exact duplicates of the evidence, also known as forensic images. This is accomplished by making a bit-for-bit copy of a piece of media as an image file with high accuracy.
Examine network traffic and logs	Attackers always leave behind traces; you just need to know how and where to look. Logs record everything that happens in an intrusion prevention system (IPS) or intrusion detection system (IDS), and in routers, firewalls, servers, desktops, mainframes, applications, databases, antivirus software, and virtual private networks (VPNs). With these logs, it is possible to extract the identity of hackers and provide necessary evidence.
Capture video	Video forensics is the method by which video is scrutinized for clues. Tools for computer forensics are used in reassembling video to be used as evidence in a court of law.
Record time offset	The format in which time is recorded against a file activity, such as file creation, deletion, last modified, and last accessed, has developed to incorporate a local time zone offset against GMT. This makes it easier for forensic examiners to determine the exact time the activity took place, even if the computer is moved from one time zone to another or if the time zone has deliberately been changed on a system.
Take hashes	Federal law enforcement agencies and federal governments maintain a list of files such as files relating to components of Microsoft® Windows® and other application software. The hash codes generated by a file or software can be compared to the list of known file hashes and hacker tools if any are flagged or marked as unknown.
Take screenshots	You should capture screenshots of each and every step of a forensic procedure, especially when you are retrieving evidence by using a forensic tool. This will ensure that data present on a compromised system is not tampered with and also provides the court with proof of your use of valid computer forensic methods while extracting the evidence.

Identify witnesses	Courts generally accept evidence if it is seconded by the testimony of a witness who observed the procedure by which the evidence was acquired. A computer forensics expert witness is someone who has experience in handling computer forensics tools and is able to establish the validity of evidence.
Track man hours and expense	When the first incidents of computer crimes occurred, it would usually take less than 40 man hours to complete a forensic investigation because incidents usually involved single, standalone computers. Now, with advances in technology and the advent of new digital media such as voice recorders, cameras, laptop computers, and mobile devices, computer forensics procedures can require a much greater amount of time and expense. Also, the increase in storage device capacities and encryption affect the amount of man hours that it can take to assess any damage, and consequently increase the expenses incurred in any computer forensics investigation. Capturing this expense is part of the overall damage assessment for the incident.

ACTIVITY 2-4: Examining Professionalism and Communication Techniques

Scenario

In this activity, you will examine different professionalism and communication techniques.

1. **What is an example of verbal communication skills? What is an example of non-verbal communication skills?**

   A: Answers will vary, but might include: For verbal communication skills, use clear, concise, and direct statements. For non-verbal communication skills, maintain the proper amount of eye contact.

2. Select the correct response.

   Which is a good example of listening skills?

   __ Maintain a neat and clean appearance.
   __ Keep sensitive customer information to yourself.
   __ Interrupt the customer to ask for more details.
   __ Let your eyes wander around the room as the customer is speaking.
   _x_ Allow the customer to complete statements without interrupting.

3. **While answering a service call on a computer that is located in a common area of the office, you come across information showing that some unauthorized websites have been viewed. The activity has been linked to a particular user account. What is the appropriate action to take?**

   A: Answers will vary, but will most likely include referring to procedures and guidelines documented by your specific organization and following the best practices used when responding to an incident, such as first response procedures, chain of custody guidelines, and documenting the entire process.

4. **When a service technician does not share sensitive customer information with others, which skill or behavior is being practiced?**

   _x_ Confidentiality
   __ Ethical behavior
   __ Respect
   __ Active listening

5. **You have received an off-site service call to service a network printer at a customer location. When you arrive, the user is at the printer and starts talking about how the printer is not working properly, and he cannot get his reports handed in on time. As a result, you start asking more clarifying questions to gather more information, so you can identify the specific issue with the printer. What type of technique are you using to gather information?**

__ Passive listening
__ Non-verbal communication
_x_ Active listening

6. **Which are examples of displaying respect during a service call?**

_x_ Asking permission before changing display settings
__ Asking "What happened just before you noticed the problem?"
__ Sitting in a user's chair without permission
_x_ Silencing your pager or mobile phone

Summary

In this lesson, you identified best practices that are followed by professional PC technicians. With the proper tools, awareness of safety and environmental issues, and basic communication skills, you are prepared to do your job in a safe, effective, and professional manner.

Which of the best practices discussed in this lesson apply in your workplace?

Have you ever been in a situation where you uncovered inappropriate conduct or prohibited activity?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 3: Peripheral Components

Lesson Time: 1 hour, 30 minutes

So far in this course, you have identified the hardware that makes up a personal computer system and examined some general best practices for working with them. Now that you have a solid base of background information, it is time to roll up your sleeves and start working with some of those hardware components. In this lesson, you will install and configure peripheral computer components.

Much of the work that you will perform as a PC technician will involve installing and configuring various hardware and software components. As an IT professional, you will often find yourself setting up end-user workstations or helping those end users with the hardware they need to make their daily lives easier. Installing and configuring peripheral components—like display devices, keyboards and mice, or even more specialized devices—are some of the more common tasks that you will perform.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Topic A:
  - Objective 1.10
- Topic B:
  - Objective 1.12
- Topic C:
  - Objective 1.4
- Topic D:
  - Objective 1.12

Topic A: Install and Configure Display Devices

In this lesson, you will install and configure peripheral components. Generally, one of the most common peripherals that you will be asked to install is the display device. In this topic, you will install and configure display devices.

The display device provides visual output from the computer system. Without the display device, you can't see any images on screen to guide your interactions with programs or see the results of your input. Correctly installing and configuring the display device enables you to meet the basic user need to see what they are working on.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.10: Given a scenario, evaluate types and features of display devices.

Display Device Types

There are several different types of display devices that you might be asked to install or configure.

Display Device	*Description*
CRT	*Cathode ray tube (CRT)* displays use electron beams within a vacuum tube to create images on a fluorescent screen. The intensity of three electron beams, one for each primary color (red, blue, and green), are manipulated to display the image on the screen. CRT monitors are larger, heavier, and boxier than their more modern counterparts due to the components used to build them, especially the thick glass used for the screen. The screen may be curved or flat, but CRTs are not considered flat-panel monitors. CRT monitors have for the most part been replaced by more modern and efficient displays like LCD, LED, or plasma screens, though many may still be in use in organizations who have yet to upgrade their devices.
LCD	Liquid crystal display (LCD) flat-panel displays are a compact, lightweight alternative to traditional CRT displays. LCDs consume much less energy than CRTs and do not emit nearly as much electromagnetic radiation as CRTs do. LCD monitors use a *cold cathode fluorescent lamp (CCFL)* as the backlight source. CCFLs use electrodes and mercury vapor to create ultraviolet light that is used as the light source. Depending on the LCD screen, the user may need to sit directly in front of the screen to see the display properly. A unique feature of LCD displays is that the screen auto centers. There is typically no center alignment needed.
LED	*Light emitting diode (LED)* displays utilize the same screen as an LCD display, but use a different backlighting technique/technology. Instead of the CCFLs used in LCD, LED screens use one of two types of light emitting diodes as a backlighting source: dynamic RGB LEDs, which are located behind the panel; or white edge-LEDs, which are located around the edge of the screen and use a diffusion panel to evenly distribute the light source. LED displays consume even less power than LCD displays. However, LED displays are currently more expensive to purchase.
	Organic light emitting diode (OLED) displays utilize the same technology as LED

OLED	displays, but use organic compounds that emit light when subjected to an electric current as the light source. However, OLED screens can be used in a larger variety of dimensions than LED screens, and are currently utilized in computer monitors, television screens, tablets, and mobile phones.
Plasma	*Plasma displays* use xenon and neon rays and a flat panel of glass to provide visuals with high contrast, brightness, and vibrant colors that can be viewed from a multitude of angles. However, plasma displays can suffer from image burn-in from repeated, long-term use. They are currently only available in very large dimensions, typically 40 inches or more, and are mostly marketed and utilized as television displays. They can also be incredibly heavy and cumbersome due to the technology.
Projector	Video projectors are often used to display the video output onto a whiteboard or other surface so that a larger audience can see it.

Other Display Devices

There are a number of other display device types that you may encounter in your personal or professional experience:

- Touch screen monitors enable input by touching images on the screen. This technology is used in bank ATMs, some point-of-sale terminals at fast food restaurants, and other situations where a separate keyboard for input is not appropriate. Touch screens are also found on many smartphones, tablets, and laptops sold for general public use.
- Virtual reality games and special-purpose imaging needs led to the development of glasses/goggles that substitute for a monitor.
- Video display systems can be used to display one image to several monitors (often used in training situations) or to display an image covering a huge screen (often used at trade shows).

Display Device Settings and Features

You can configure several features and settings for a display device, either through the **Control Panel** utility in the Windows® system or through controls on the physical device.

Display Setting or Feature	***Description***
Resolution	The number of *pixels* that make up the dimensions of a display. The resolution value is given as the number of horizontal pixels by vertical pixels, or width by height, traditionally in the ratio of 4:3. For wide screen displays, the ratio is 16:10. Common resolutions are 640 x 480, 800 x 600, 1024 x 768, and 1600 x 1200. The higher the resolution, the more objects or information you can fit on the screen at once. Just as widescreen televisions have become popular, video monitors with higher aspect ratio are also becoming more common.
Native resolution	A fixed resolution for LCD or other flat panel display devices. Unlike a CRT, which can change resolution to match that of the signal being received, display devices with native resolution will only display the best quality image when the input signal and the native resolution are the same. Other resolutions may display on a device where that signal input is not the same as the native resolution, but it will result in image quality loss.
Refresh rate	The number of times per second that the entire monitor is "refreshed," or scanned to illuminate the pixels. Each scan is referred to as a frame. The rate is expressed in *hertz (Hz)*. Typical refresh rates are 60 to 70 Hz or 60 to 70 times per second. Any setting lower than 60 Hz usually produces noticeable flickering.
Brightness	The amount of light that is being emitted from a display device. Brightness is measured in *lumens*, which is the unit of measurement for visible light that is being emitted from a light source. On a display device, brightness can be increased or decreased for the display. If the brightness is set too high, you might get an "aura" effect displayed on the screen. If it is set too low, you might not see anything on the screen.
	Many users choose to use more than one display device to increase the amount of display space. The typical setup is two displays, though more than two displays can be configured with the appropriate expansion card that can support that setup. Multiple displays are most commonly used for either a professional computer workstation or for gaming environments, where an extended desktop is useful.

Multiple displays	Within the monitor's display properties, you can designate one of the two monitors as the primary monitor, which controls where the desktop administrative features (**Start** menu, taskbar, etc.) appear. The other monitor would contain extra desktop space. While it is far more common to have the desktop span both monitors and contain a different window in each, it is also possible to have the two monitors display the same image, which is useful for presentations.
Analog vs. digital	Depending on the type and make of the display device, it may support either analog or digital inputs. Most devices providing the input signals (like a computer) are inherently digital. CRT display devices are analog, and will need a video card and VGA cable to receive the digital input and convert it to analog. Newer display devices such as LCD or LED can innately support digital input signals, and do so via Digital Video Interface (DVI) connections between the input device and the display device.
Privacy/antiglare filters	Privacy or antiglare filters are physical accessory screens that can be attached onto or over a display device and provides a number of benefits: • Reduces glare from the screen for the user sitting in front of the display device. • Protects the display device screen from scratches or dust. • Prohibits others not sitting in the front of the device from viewing information being displayed, protecting confidentiality and providing privacy.
Color depth (quality)	The number of bits used to store the color of a pixel: the more bits per pixel, the more colors can be displayed.
Font	A size and style of typeface. Computers use fonts to display text on the screen. Common font faces include Arial (which is a sans serif font), Times (which is a serif font), and Courier (which looks like legacy computer output).
Contrast	The difference in intensity between adjacent colors in an image. If the contrast is not set correctly for the display device and the lighting conditions in the room (for example, a really bright or really dark room), you might not be able to see anything on the screen, or you might get strange results.
Image position	The location or size of the display in relation to the physical device. Sometimes the image is not centered on the display screen. Other times the image does not fill the screen, leaving a black band around the edge. Or, part of the image can scroll off the screen. There are usually separate buttons or menu options to adjust each of these issues.
	Distortions can appears as curves, waves, or moiré patterns in the video image. These are typically caused by electromagnetic interference or a defect with hardware, usually with the video card or video cable. If lines do not appear straight

Distortion control	on the screen, you might need to adjust settings. Electromagnetic issues, however, are resolved by eliminating the source of interference. Refer to the display device documentation for how to resolve such issues. Distortion control is configured on the display device itself, not through a system utility.

Aspect Ratio

The aspect ratio is the ratio of width to height of a display. Most software expects a 4:3 ratio, and the display will appear to be distorted if other ratios are used. The aspect ratio is found by determining the proportion of the number of pixels across the screen to the number of pixels down the screen. For example, a resolution of 640 x 480 has a 4:3 aspect ratio.

Resolution	***Number of Pixels***	***Aspect Ratio***
320 x 200	64,000	8:5
640 x 480	307,200	4:3
800 x 600	480,000	4:3
1,024 x 768	786,432	4:3
1,280 x 1,024	1,310,720	5:4
1,600 x 1,200	1,920,000	4:3

LearnTO: For a demonstration, check out LearnTO **Adjust Display Output Settings** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Device Drivers

A *device driver* is a type of software that enables the operating system and a peripheral device to communicate with each other. Also referred to as simply a driver, a device driver takes generalized commands from the system software or an application and translates them into unique programming commands that the device can understand. It also provides the code that allows the device to function with the operating system, and it is generally installed as part of the installation process for a new piece of hardware. Device drivers can be generic for a class of device or specific to a particular device.

Where to Get Device Drivers

Device drivers can be:

- Included with the operating system. New operating systems include thousands of drivers that allow them to work with all current, popular devices. Peripherals that are designed after the operating system comes out must supply their own drivers.
- Supplied with the device on a CD-ROM when you purchase the hardware.
- Downloaded from the Internet from an operating systems vendor's site, such as Windows Update, or from the hardware manufacturer’s website.

Display Device Selection Tips

There are hundreds, if not more, of display devices from which you can choose, depending on your needs. Selecting the display device to use may depend on a number of things.

Criteria	*Description*
Size	Depending on the space available for the display or a user's personal preferences, you may choose a display based on the physical size or footprint of the device. Because they take up less space, flat-panel devices like LCD, LED or OLED, may be preferred or needed for small work spaces. Plasma screens are still rather large, and may not be practical for a workstation.
Technical needs	Depending on what the display device will be used for, technical requirements for programs, or personal preferences, a specific type of display device may be required or desired. LCD, LED/OLED, and plasma monitors support high resolutions, which make them a better choice for users who work in high-end graphics applications such as Adobe® Photoshop®. However, some users still prefer CRT monitors because their display is brighter.
Efficiency	As the technology used in display devices evolves, the devices tend to be more energy efficient than its predecessors. LEDs consume less energy than LCDs, which may make them preferable if you are trying to be more energy efficient and cost efficient.
Cost	The newer the technology, the more expensive the device. LCDs are still fairly low cost, as the most common and in-demand type of display. LEDs and OLEDs are more expensive, but as they become more common, the cost is decreasing as well. Plasma displays are currently the most expensive option.

Display Device Installation Considerations

When you are ready to install a display device, keep the following considerations in mind:

- Do you have the necessary cables and connectors available to connect the display device to the machine?
- Do you have the necessary expansion cards, such as a video card, installed on the machine to support the display device you have selected?
- Do you have the necessary drivers for the display device installed on the machine?
- Do you have a power source available for the display device?

LearnTO: For a demonstration, check out LearnTO **Install a Display Device** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Display Devices**

ACTIVITY 3-1: Examining Display Devices

Scenario

In this activity, you will examine display devices.

Examining Display Devices

1. **What step should you complete first when you are installing a monitor?**

   __ Secure the monitor to the port by tightening the screws on each side of the connector.
   _x_ Turn off the computer.
   __ Plug in the monitor power cord.
   __ Locate the monitor port on the computer.
   __ Align the pins on the monitor cable with the holes in the adapter port and plug in the monitor.

2. **What kind of video is component video?**

   _x_ Analog
   __ Digital
   __ HD
   __ Brightness only

ACTIVITY 3-2: Installing Display Devices

Before You Begin

You have a working monitor with either a 15-pin VGA-style monitor cable and a computer equipped with a VGA port or you have a digital flat-panel monitor (LCD or LED) that uses the 29-pin DVI connector, High-Definition Multimedia Interface (HDMI) connector, or a universal serial bus (USB) display. The computer is turned off and the monitor is unplugged.

Scenario

The marketing department of your company is moving to new offices, and you have been assigned the task of setting up the computers in their new offices. The computers and monitors have been delivered to each office. Employees want to begin using their computers as soon as possible.

1. Install the monitor.
    a. Verify that the power is off at the computer.
    b. Locate the monitor cable and examine the connector.
    c. If you have a standard VGA CRT monitor, locate the VGA adapter port on the computer. If you have an LCD display, locate the VGA, 29-pin DVI, or the USB port on the computer.
    d. Insert the monitor connector into the appropriate port, being sure to align the pins carefully.
    e. Tighten the screws. Do not over-tighten them.
    f. Plug in the monitor.
2. Check whether the monitor is functional.
    a. Turn on the computer power.
    b. Turn on the monitor power.
    c. After the system has started to boot, verify that the power light on the monitor is green and is not flashing.
    d. Watch the monitor and verify that the display is clear.

ACTIVITY 3-3: Configuring Display Devices

Before You Begin

Every computer in the physical classroom is assigned a unique computer name. Some steps in the activities refer to computer names such as **Admin**##, where ## refers to a student's number. A student whose number is 01 should enter ***Admin01*** as the user name on his or her computer, a student whose number is 02 should enter ***Admin02*** as the user name, and so on. The password is ***!Pass1234*** and is the same for each user.

Setup

Your instructor has altered the display settings for your monitor. The computer is running and the **Welcome** screen is displayed.

Scenario

An employee recently had to move the location of his workstation. The employee reports that, since the move, the display does not appear in the center of the monitor. The images are too dark, making them difficult to see, and he cannot see as much on the screen as he would like. The employee needs you to resolve these issues so that he can get back to work.

1. Adjust the monitor display.
    a. Referring to the monitor's documentation as necessary, locate the physical controls to adjust the brightness of the display image.
    b. Adjust the brightness so that the monitor is comfortable to view.
    c. Adjust the contrast so that you can view all the screen elements easily.
2. Change the resolution.
    a. To open the Screen Resolution window, right-click the desktop and select **Screen resolution.**
    b. In the **Resolution** section, select the current resolution to display the drop-down list.
    c. In the Screen Resolution window, drag the slider or click to select the appropriate resolution.
    d. Select **OK.**
    e. In the **Display Settings** message box, select **Keep changes** to set the new resolution.
3. Adjust the horizontal and vertical positions of the image.
    a. Referring to the documentation as necessary, locate the controls to adjust the size and centering of the display image.
    b. Adjust the vertical display position so that the display is centered top-to-bottom on the screen.
    c. Adjust the horizontal display position so that the display is centered side-to-side on the screen.
    d. Adjust the height and width of the image so that there is either no border or the smallest

border allowed.

Topic B: Install and Configure Input Devices

In the previous topic, you examined display devices and how to install and configure them so that users can see the computer system's output. Users also need to be able to interact with the computer system by using input devices. In this topic, you will install and configure input devices.

Computers need user input such as directions or commands and user interaction with the programs that are included in order to produce something of use. Keyboards and pointing devices are the standard input devices for personal computers these days, but there is an ever-growing number of input devices available for the user to interact with in a variety of ways. As an A+ technician, part of your responsibilities will include installing and configuring all types of input devices.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.12: Install and configure various peripheral devices.

Standard Input Device Types

Common input devices include mice and keyboards, but even these two components come in a variety of implementations.

Input Device	*Description*
Standard keyboard	Standard keyboards are rectangular in shape, and have 84, 101, or 104 keys. • The original PC keyboard, the XT, has 84 keys. A numeric pad is integrated to the right of the alphabetical keys. Function keys are along the left side of the keyboard. • The AT keyboard also has 84 keys and is very similar to the original PC keyboard. However, on the AT keyboard, the numeric pad is separate from the alphabetical keys. • The AT Enhanced keyboard has 101 keys. The function keys are integrated across the top. Arrow keys have been added, as well as a set of six keys—**Insert, Delete, Home, End, Page Up,** and **Page Down.** There are also additional command keys such as **Esc** and **Ctrl.** • The Windows 104-key keyboard is similar to the AT Enhanced keyboard, but adds two **Windows** keys and a **Menu** key. The **Windows** keys are analogous to clicking the Windows **Start** button and the **Menu** key performs the same functions as right-clicking the mouse.
Ergonomic keyboard	Natural or ergonomic keyboards usually split the keyboard in half so each hand can comfortably use its own set of keys. Built-in wrist rests are common, and some ergonomic keyboards also have an integrated pointing device such as a trackball or touch pad.
Dvorak keyboard	Dvorak keyboards rearrange the keys into a more efficient arrangement that makes faster typing possible for users who have become familiar with it.
Mouse	A mouse is a small object that runs across a flat surface and has at least one, but typically two or three, buttons that send electronic signals to the graphical user interface (GUI). Its name is derived from its appearance—a small rounded rectangle shape with a single cord attached at one end. Mice can be: • Mechanical—A ball on the underside runs along a flat surface. Mechanical rollers

	detect the direction the ball is rolling and move the screen pointer accordingly. • Optical—A laser detects the mouse's movement. Optical mice have no mechanical moving parts, and they respond more quickly and precisely than other types of mice.
Trackball mouse 	A trackball is basically an upside down mouse. The ball is mounted on the top of the case instead of the bottom and signals are sent to the computer by moving the ball with your thumb, fingers, or palm instead of by rolling the ball across a flat surface. Like a mouse, a trackball has at least one button that is used to send electronic signals to the computer.
Touch pad 	A touch pad is a small, touch-sensitive pad where you run your finger across the surface to send electronic signals to the computer to control the pointer on the screen. Touch pads can have buttons like a mouse or trackball, or the touch pad can be configured to detect finger taps on its surface and process those signals like button clicks.
Trackpoint 	A *trackpoint*, or pointing stick, is most commonly found on laptops. Located in the center of the keyboard, the trackpoint is a small joystick-like button that responds to user force in all directions in order to move the mouse pointer on screen.

Specialty Keyboards

Specialty keyboards include:

- Keyboards for children or users with special needs. These may have enlarged or specially constructed keys.
- Foreign language keyboards, which have a variety of different keys.
- Custom application keyboards, which can have multimedia access buttons, video/audio editing software buttons, and gaming devices.

Ports, Cables, and Connections

Keyboards and mice can use several types of ports and connections:

- Serial (now largely obsolete)
- Standard DIN (5-pin, and largely obsolete)
- PS/2 (6-pin mini-DIN)

- USB
- Wireless infrared
- Wireless radio frequency (RF)
- Bluetooth

Function Keys

Function keys, typically positioned horizontally along the top length of the keyboard, allow a user to do two things: they launch operating system commands, and they allow a user to customize the input from the keyboard. For example, when booting a PC, a user can change Basic Input/Output System (BIOS) settings by choosing certain function keys. A user can also customize how certain programs interpret function keys. On smaller devices, such as laptops, a user might notice a key labeled "Fn." This key is usually labeled in a different color from the rest of the keyboard, and is used in conjunction with other keys to increase the number of distinct inputs a keyboard can offer. Many of the **Fn** inputs control video or sound settings since there are not usually separate monitor buttons on a laptop.

Biometric Input Device Types

Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic unique to the individual, such as a retina pattern, fingerprint, or voice pattern. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric input devices can add an additional layer of physical security or information security by verifying the identity of the person attempting to gain access to a location or device.

Several types of biometric input devices might be used in an organization.

Biometric Device	***Description***
Fingerprint scanner/reader 	Scans a person's fingerprint(s) and matches it against a database of fingerprints to verify that person's identity. Once verified, that person will be able to access a building, location, or device or can be used with point-of-sale applications to complete a transaction. If not hard-wired into a system (such as a security system), fingerprint scanners/readers used with smaller devices like a personal computer typically connect via a USB connection. Some laptops have a fingerprint scanner integrated into the system as well, which is usually placed near the keyboard area of the laptop. The scanner is used to verify the identity of the user and grant them the ability to use the laptop.
Retina scanner 	Scans a person's retina or iris and matches it against a database of retina scans to verify the person's identity. Once verified, that person will be able to access a building, location, or device. If not hard-wired into a system (such as a security system), a retina scanner used with a smaller device like a personal computer typically connects via a USB connection.
Voice recognition	Uses a spoken phrase called the "pass phrase" and compares it against a person's "voice print," a recorded and stored version of that person saying the pass phrase, to verify identity. Once verified, that person will be able to access a building, location, or device.

	If not hard-wired into a system (such as a security system), a voice recognition system used with a smaller device like a personal computer typically connects via a USB connection.
Signature recognition 	Uses a signature pad and a database of approved signatures. A user signs the signature pad, and the recognition system analyzes the individual behavior of the person signing, such as the strokes used and the pressure applied while signing, to verify the identity of the user. If not hard-wired into a system (such as a security system), a signature capture pad used with a smaller device like a personal computer typically connects via a USB connection.
Keyboard 	Using a biometric keyboard, only authorized users would be able to use the keyboard, and only once their identity was verified through the verification program. The keyboard and a special program monitor the individual's typing behaviors, such as key press duration or pressure, key strokes, and so forth, to create a baseline for normal typing for the individual. The program can challenge a user to verify identity by typing, and compares the keystroke behavior of the typist to that stored in a database for the user. Most biometric keyboards connect via a USB connection.
Mouse 	Using a biometric mouse, only authorized users would be able to use the mouse and access or navigate the computer system, and only once their identity was verified through the verification program. A biometric mouse uses biometric authentication, typically a built-in fingerprint reader, to verify the identity of the user and provide them control over the mouse. Most biometric mice connect via a USB connection.
Storage devices 	Using a biometric storage device, such as flash drive or hard drive, only authorized users would be able to access files or data stored on the storage device. Biometric flash drives or hard drives use another kind of biometric authentication, typically a built-in fingerprint reader, to verify the identity of the user and provide them access to the flash drive files. Most biometric storage devices connect via a USB connection.

Biometric devices will need to be installed and configured, and then initialized for the specific end user that will be using the device. The initial biometric authentication “object” for the user (be it a fingerprint, retina scan, pass phrase, etc.) must first be captured and stored. Then the user will have to test the device to make sure that it accurately verifies his or her identity against the authentication object, permitting them access to the location or device.

Specialized Input Device Types

Although keyboards and mice are the most popular of the input devices for personal computers, there are some specialized input devices that you might encounter in your workplace.

Input Device	*Description*
Touch screen	Touch screens enable users to enter inputs by touching areas on a monitor screen. They can be activated by a finger touch or a stylus touch. Touch screens are composed of: • Touch sensors. The sensors can be a panel that lays over a standard monitor or can be built into a special touch screen monitor where the user actually touches the glass on the monitor. • A controller. If using an overlay panel, the controller connects to the panel and then to a PC port. Many use a COM or USB port, although there are special instances where the controller connects to a drive or other device or port. For touch screens with built-in touch sensors, the controller is built into the monitor. In this case, the monitor contains two cables—one to the monitor port and one to the COM or USB port (or other port). • A device driver or specialized software. This enables the operating system to receive and interpret information from the touch screen device.
Scanner	A scanner is used to take a photo-identical copy (scan) of a physical hard copy of any kind of document, such as a piece of paper or a photo, and create a digital-format copy of the document. A scanner is similar to a photocopy machine or copier, but with a much smaller footprint. Scanners can be attached directly to a personal computer to import scanned copies of documents. With the proper software or program installed, scanned versions can be manipulated and edited once they have been imported. A scanner typically uses a USB or high-speed USB connection to connect between devices.
Barcode	Barcodes provide a simple and inexpensive method of encoding text information that is easily read by inexpensive electronic readers. A barcode reader decodes a barcode by scanning a light source across the barcode and converting the pattern of reflected light to an electronic signal that is decoded back to the original data by electronic circuits. There are currently four different types of barcode readers available: pen-type readers

reader	(or barcode wands), laser scanners, Charge Coupled Device (CCD) readers, and camera-based readers. Barcode scanners or readers connect to a device via a USB connection or are wireless.
Microphone	Microphones record any type of sound and convert it to a electronic or digital format. Once in this format, the recorded sounds can be manipulated or edited, and used in a variety of ways. Microphones typically connect to a device through a dedicated Mic jack, but some connect with a USB connection. Some laptops may have a built-in microphone.
Gamepad	A gamepad is a game controller used to interact with a video game console or program, typically held and manipulated with two hands. It uses a number of buttons and toggles, each of which controls a different action within the game program. The latest versions of many gamepads also include sensors and pointing devices that sense directions of movement and rotation, and use a combination of these movements to control actions within the game program. Gamepads typically connect to a device via a USB connection. The latest technology in gamepads is unique in its wireless capabilities: many gamepads do not attach to a device via a connector, but rather transmit inputs wirelessly to the receiving device or console.
Joystick	A joystick is a pivoting stick or lever attached to a base that is used to control movement on a device. It typically also includes push buttons, toggles, or switches that control other actions associated with the program or device that the input is controlling. The joystick inputs the angle and direction of a desired movement. Joysticks are most commonly used to control video games or other computer programs, but are also used to control machines and devices such as cranes and unmanned vehicles. Legacy joysticks connected to a computer via a game port, a device port designed specifically for connecting this input device. However, most modern joysticks connect to the device via a USB connection.
Digitizer	A digitizer is any device that performs digitization, which is the conversion of any type of analog signal into its digital form. This includes images, objects, text, and so forth. However, the term is most commonly used in reference to the device used to convert audio and video data into a digital format that can be edited, manipulated, and viewed

	on a computer, television or other device. A digitizer typically uses a USB or high speed USB connection to connect between devices. Some older versions may use an S-Video and Composite-to-USB connection.
Interactive whiteboard	An interactive whiteboard looks similar to a traditional whiteboard; however, it connects to a computer using a wired USB cable, or connects wirelessly through a Bluetooth® connection. A projector is typically used with it to display the computer's desktop, and it can be used as an input device once the correct device drivers are installed on the computer. You can manipulate the computer directly on the whiteboard using a special stylus or by using your finger. Interactive whiteboards are used in many schools today, and have become a very popular teaching tool.

Touch Screen Technologies

Touch screens can gather input through a number of different technologies:

- Capacitive: Uses electrical conductors to manipulate the screen. The screen is coated with a conductor and, as the human body is also a conductor, contact on the surface of the screen by a finger or other body part results in a change to the screen's electrostatic field. The change in the field provides a horizontal and vertical coordinate, pinpointing the location of the touch on the screen.

- Resistive: Uses electrically resistive layers to comprise the screen. When the touch object (finger or stylus) pushes down on the first outer layer, it depresses and touches the second layer, creating an electrical charge between the two layers that provides a horizontal and vertical coordinate, determining the location of the touch on the screen.

- Surface Acoustic Wave: Uses ultrasonic waves that are disrupted when the screen is touched. The change in the wave is absorbed and registers where the screen was touched, determining the location of the touch on the screen.

- Infrared: Uses infrared LEDs and photodetectors that are disrupted when the screen is touched. The LED beams are set up in a cross-hatch pattern that are disrupted when the screen is touched, and determine the location of the touch on the screen.

- Optical imaging: Uses image sensors placed around the screen that detect the touch on the screen based on the shadow that is created when the screen is touched. The image sensors compare the information about the shadow to determine the location of the touch on the screen.

- Dispersive signal: Uses sensors that detect vibrations that occur when the screen is touched. The vibrations created by the touch are analyzed to determine the location of the touch on the screen.

- Acoustic pulse recognition: Uses unique acoustic sounds that are associated with a specific

location on the screen to determine the exact location of the touch on the screen.

Specialized Input Devices in Everyday Life

Many people might encounter specialized input devices during a trip to the grocery store. It is increasingly common to see the cashier use a barcode scanner to account for the item's price, and to use a touch screen to enter any additional information (such as whether there is more than one item at that price, or to enter the correct produce code). Additionally, most grocery stores use a touch screen device to capture the customer's credit card number and accept any additional user input, such as a PIN. Finally, the touch screen device often has a stylus attached so that the customer can sign the screen; there will be no paper at all in this entire transaction.

KVM Switches

A *keyboard, video, mouse (KVM) switch* is a device that enables a computer user to control multiple computers with a single keyboard and mouse, with the display sent to a single monitor. This feature is particularly useful in managing multiple test environments, or in accessing multiple servers that have no need for dedicated display or input devices. KVM switches are available with PS/2 or USB connections, and come in desktop, inline, or rack-mount varieties. Higher-end rack-mount models can be uplinked to connect dozens of computers.

Figure: A KVM switch.

Input Device Selection Tips

Windows operating systems support a variety of input devices, so you should select an input device based on user requirements.

Input Device	*Description*
Keyboard	When selecting a keyboard for a user, in addition to considering its ergonomics, you should also consider whether the keyboard offers additional features (such as customizable hot keys and scrolling) as well as wireless connectivity. Many users now prefer to use a wireless keyboard as it gives them the freedom to locate the keyboard anywhere on their desks. In some cases, users might be able to use a Bluetooth-enabled keyboard to communicate with both their desktop computers and a mobile device such as a tablet or a smartphone. Be sure to determine the potential keyboard's connector requirements; if the keyboard uses USB, you will need to make sure the user's computer has an available USB port.
Pointing device	When selecting a mouse for a user, most users prefer optical mice because they are less susceptible to problems such as dirt interfering with the rollerball. As with keyboards, you will also find that users prefer wireless mice over wired mice because of the freedom it gives them to move around while working. Besides these factors, choosing between a mouse, a trackball, and a touch pad comes down to the personal preference of the user.
Biometric device	Whether or not a biometric device is being deployed will likely be a decision made based on an organizational security policy or standard. If biometric devices will be deployed at individual workstations, you will need to determine the specific biometric device's connector requirements; as most use a USB connection, you will need to make sure that the user's computer has an available USB port to connect the device.
Specialty device	Using a specialty device will be determined by two main factors: is the device needed by the end user as a matter of productivity (to complete job tasks)? Or is the device desired by the end user as a personal preference? If any specialty devices will be deployed on the system, you will need to determine the device's connector requirements. Most specialty input devices use a USB connection, so you will need to make sure that the user's computer has an available USB port or ports if multiple specialty devices will be connected.

Input Device Installation Considerations

Before you attempt to install an input device, you should consider certain factors.

Factor	*Considerations*
Drivers	Be sure that you have the most current drivers for the input device for the operating system of the computer on which you plan to install it. If you install a USB device, you might get a HID message (which stands for "Human Input Device"). Either let the PC find the right driver, or restart the computer and see if the issue resolves itself. If that does not work, you will need to find a driver for the device.
Ports	Make sure that the computer has an available port to which you can connect the device. Input devices can use a variety of ports, including PS/2, serial, parallel, USB, infrared, and FireWire/IEEE 1394. If a large number of input devices will be connected using the same connector type, you may need to consider using a hub, splitter, or extender that creates multiple accessible ports via one port on the device. For example, a USB hub expands one USB port into several available USB ports, using an upstream port that connects to the device USB port and multiple downstream ports on the hub.
Manufacturer's instructions	Review the manual or quick start guide that came with the device. In some cases, the manufacturer might require you to install the device drivers before connecting the device to the computer.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Input Devices**

ACTIVITY 3-4: Installing Input Devices

Before You Begin

For this activity, you will need a replacement keyboard and mouse or other pointing device.

Scenario

You have received a service call to replace a user's mouse and keyboard.

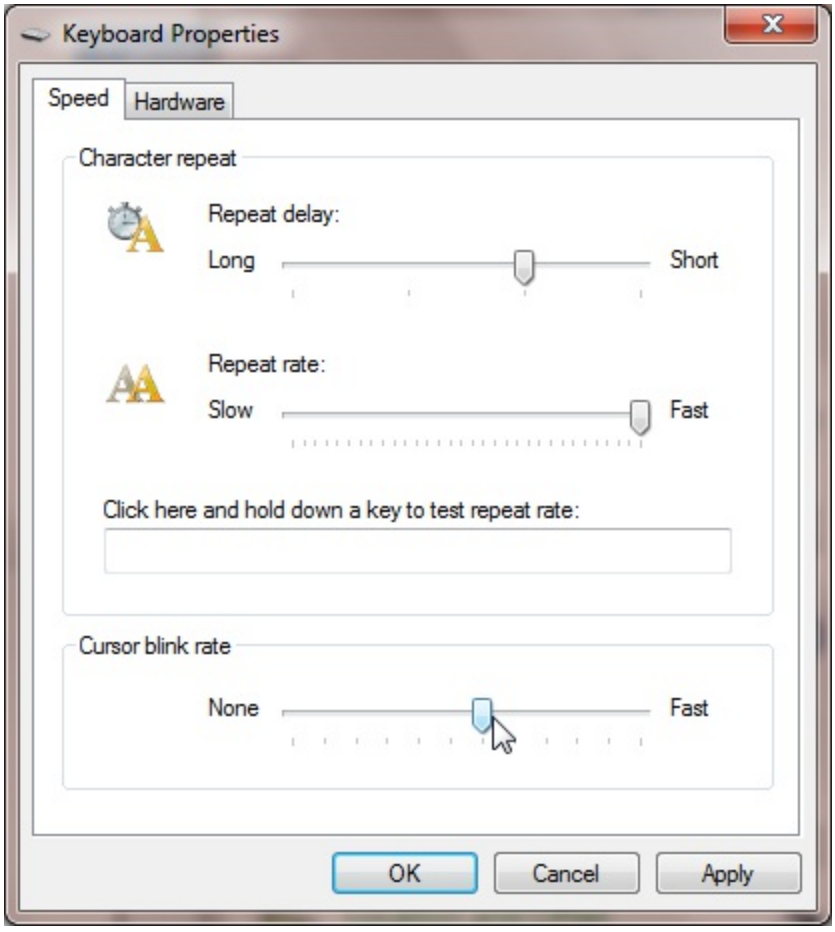
1. Replace the keyboard.
    a. Shut down the computer.
    b. Determine the connection type used by the replacement keyboard.
    c. Unplug the old keyboard from the system unit.
    d. Plug the new keyboard into the appropriate PS/2 or USB port.
2. Replace the mouse or pointing device.
    a. Determine the connection type used by the replacement mouse.
    b. Unplug the old mouse from the system unit.
    c. Plug the new mouse into the appropriate PS/2 or USB port.
    d. Start the computer.
3. Test the installed devices.
    a. Use the keyboard to access the **Start** menu.
    b. Move the mouse around to verify that it is working properly.

ACTIVITY 3-5: Configuring Input Devices

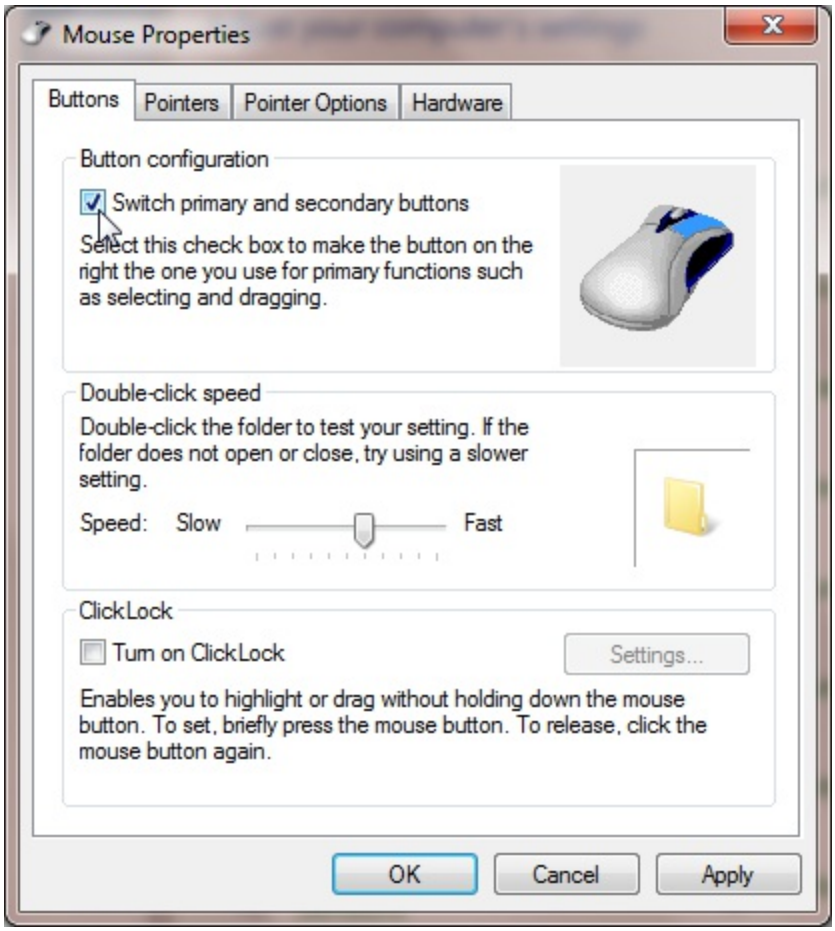
Scenario

You just replaced a user's mouse and keyboard. The user is left-handed and prefers a slow-blinking cursor. She also has a hard time distinguishing the mouse pointer from other screen elements, and asks if you can adjust the pointer to something more easily discernible.

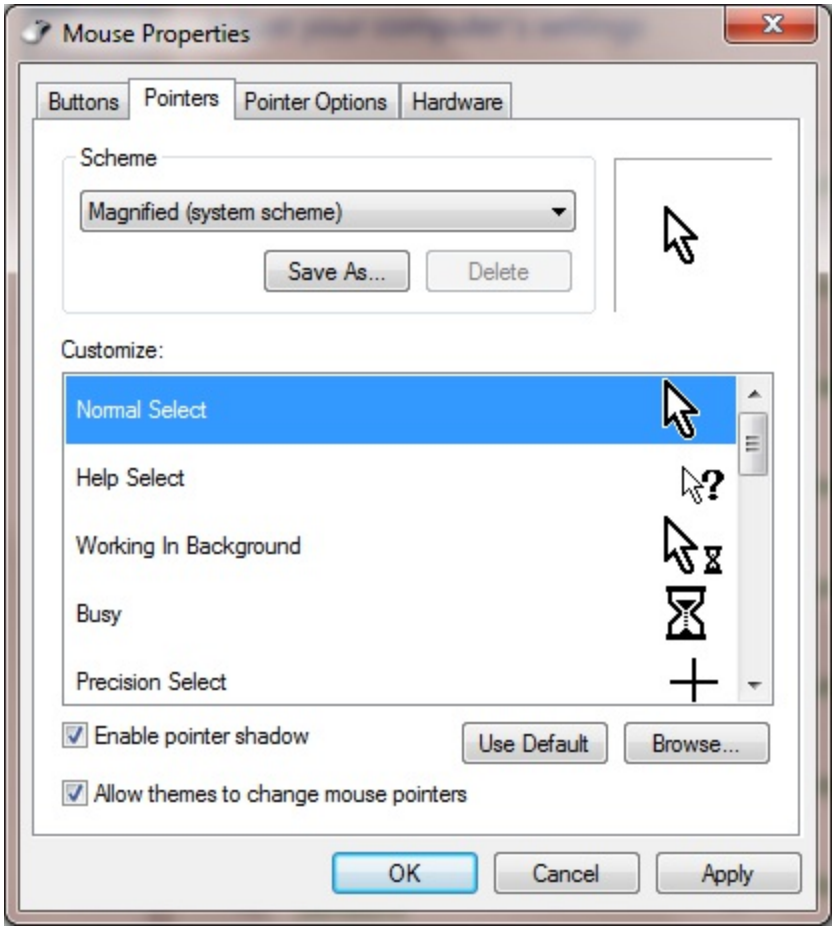
1. Configure the keyboard settings.
   a. Select **Start→Control Panel.**
   b. In the Control Panel window, in the **Adjust your computer's settings** section, from the **View by** drop-down list, select **Large icons.**
   c. Select the **Keyboard** link.
   d. In the **Keyboard Properties** dialog box, on the **Speed** tab, reduce the cursor blink rate by dragging the **Cursor blink rate** slider to the left.



   e. Select **Apply.**
   f. Select **OK.**
2. Configure the mouse settings.
   a. In the Control Panel window, select the **Mouse** link.
   b. In the **Mouse Properties** dialog box, on the **Buttons** tab, check the **Switch primary and secondary buttons** check box.


Mouse Properties
Buttons
Pointers
Pointer Options
Hardware
Button configuration
Switch primary and secondary buttons
Select this check box to make the button on the right the one you use for primary functions such as selecting and dragging.
Double-click speed
Double-click the folder to test your setting. If the folder does not open or close, try using a slower setting.
Speed:
Slow
Fast
ClickLock
Turn on ClickLock
Settings...
Enables you to highlight or drag without holding down the mouse button. To set, briefly press the mouse button. To release, click the mouse button again.
OK
Cancel
Apply

c. To verify that the right mouse button is now the primary button, right-click the **Pointers** tab.
d. Right-click the **Buttons** tab.
e. Select the **Pointers** tab.
f. From the **Scheme** drop-down list, select **Magnified (system scheme).**



g. Select **OK.**

3. Reconfigure the mouse settings to suit your personal preferences, and close the **Control Panel**.

Topic C: Install and Configure Expansion Cards

In the previous topic, you installed input devices, such as mice and keyboards, that are most commonly connected and used on a computer system. These devices typically connect using standard ports that are available on most machines, such as a USB port. You can expand the functionality of your computer by adding expansion cards that provide additional ports for a variety of peripheral devices. In this topic, you will install and configure expansion cards.

Display devices, keyboards, and other pointing devices are the most common devices you are likely to install and configure; these devices are typically included in a standard workstation environment when a PC is requested. When a user needs to connect a peripheral component that doesn't have an existing interface, like a multimedia device, you will need to install an expansion card. As an A+ technician, your responsibilities are likely to include upgrading users' computers by installing a variety of components, including expansion cards.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.4: Install and configure expansion cards.

Expansion Card Types

Expansion cards extend the capabilities of a computer. There are many different types of expansion cards, each of which provide different capabilities.

Expansion Card Type	***Description***
Sound cards	A sound card or audio card provides the interface necessary for the input and output of audio signals both to and from the computer.
Video cards	A video card, sometimes called a display card or graphics card, provides the interface necessary to generate the visual output that is sent to the display device.
Network cards	A network card, sometimes called a network interface card (NIC), provides the interface necessary for network communications, whether for wired or wireless connectivity.
Serial and parallel cards	A serial or parallel card provides the interface necessary for the computer to recognize and interact with any devices that connect to the computer via a serial or parallel connection. Devices that utilize serial or parallel connections include modems, display devices, barcode scanners, point of sale devices, and more.
USB cards	A USB card provides the interface necessary for the computer to recognize and interact with all devices that connect to the computer via a USB connection. Devices that utilize USB connections include keyboards, flash drives, cameras, and more.
FireWire cards	A FireWire card provides the interface necessary for the computer to recognize and interact with all devices that connect to the computer via a FireWire connection. FireWire is mainly used for high-speed data transfer. Devices that use FireWire connections include external hard drives, video and audio recording devices, and more.
Storage cards	A storage card provides the interface for the computer to recognize and interact with a storage device such as a disk. Systems with multiple disk drives, especially of different types, may require multiple storage cards to manage the communication between the disks and the system board.
Modem cards	A modem card provides the interface necessary for remote communications over phone or data lines that have been provided by a cable or Internet service provider.
Wireless/cellular cards	A wireless or cellular card provides the interface necessary for remote communications, such as Internet over mobile phone or wireless data lines such as Wi-Fi, 3G, or 4G Internet that have been provided by a cellular service provider.
TV tuner cards	A TV tuner card provides the interface necessary for the computer to receive television signals and display the output on a display device.
Video capture cards	A video capture card provides the interface necessary for the computer to input video feeds, including digital video, and interact with the software necessary to process and edit video.
Riser cards	A riser card provides the interface necessary for adding expansion cards to a system board while saving space within the system case. A riser card allows the

	cards to stack horizontally rather than vertically within the system.

Extended Capabilities for Sound Cards

Because so many computer manufacturers now build sound capabilities into motherboards, many sound card manufacturers add extended features to their cards in order to justify their purchase. These features might include digital output so that you can integrate the computer into a home entertainment system, or FireWire connections so that you can play MP3 recordings directly from an MP3 device.

Card Selection Tips

Before selecting an expansion card for a computer, you must verify that its bus type is compatible with the computer. In addition, you must also make sure that the expansion card's drivers are compatible with the computer's operating system. Typically, most expansion cards on the market today support Plug and Play (PnP) standards. PnP is a functionality of many buses that automatically detects new hardware, and automatically assigns resources for the device, without the need for manual configuration. If you plan on using PnP when adding expansion cards, make sure that the computer's BIOS and operating system support it.

Card Installation Considerations

Before you attempt to install an expansion card, verify that the computer has an available slot that matches the expansion card's bus type and that you have the device's latest drivers for the computer's operating system. Be sure to unplug the computer and discharge any static electricity before installing the card. If you are installing a card that has its own cooling system, such as a fan, make sure there is enough room for the card's airflow system to function properly.

Expansion Card Configuration

Once the expansion card is installed, there are a number of means for configuring the expansion card. Depending on the type and manufacturer, you may need to use one or a combination of these methods.

Configuration Method	*Description*
PnP installation	If the expansion card, the device, the BIOS, and the operating system (Windows® 95 and newer) are all PnP compatible, the expansion card will be automatically configured and the system will automatically assign resources to the card when the system starts.
Manufacturer driver	If Windows does not automatically detect an expansion card, you can manually install a driver from the manufacturer.
The **Add Hardware** wizard	You can use the **Add Hardware** wizard to install and configure PnP devices, although to install most unrecognized devices, you will typically just run a setup program provided by the manufacturer.
Hardware scan	When using the wizard, you should initially let Windows try to scan for new hardware (this is the default selection).
Device list	If Windows cannot find the device, you can then choose the device from a list of devices offered by Windows and Windows will install the appropriate driver.

Installation Instructions

Note: Read the installation instructions for the expansion card to determine if any software is required prior to the installation. Failure to do so could cause the installation to fail or the card and system to behave erratically.

LearnTO: For additional information, check out LearnTO **Install Expansion Cards** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Expansion Cards**

ACTIVITY 3-6: Examining Expansion Cards

Scenario

In this activity, you will examine expansion cards.

Examining Expansion Cards

1. **Which expansion card provides interfaces necessary to connect Small Computer Systems Interface (SCSI) devices?**

   _x_ Input/output card
   __ Multimedia card
   __ Video card
   __ Modem card

2. **True or False? Before attempting to install an expansion card, verify that the computer has an available slot that matches the expansion card's bus type.**

   _x_ True
   __ False

3. **What is the first step in installing an expansion card?**

   __ Turn off power to the system and unplug the power and peripheral cables.
   __ Remove the system cover and access the slots on the system board.
   __ Remove the slot cover from an empty slot.
   _x_ Read the quick start guide to see if drivers or other software should be installed before or after installing the card.

ACTIVITY 3-7: Installing Expansion Cards

Before You Begin

You have open expansion slots on the system board. You have been given one or more expansion card types and device drivers.

Scenario

You have been asked to install several expansion cards on a user's system. The appropriate drivers for the cards are also available to you should you need them.

1. Open the system cover and access the slots.
   a. Turn off the system power.
   b. Unplug the computer from the electrical outlet.
   c. Unplug peripherals from the system.
   d. Remove the cover.
   e. Determine if you need to move or remove any components in order to access the slots.
2. Insert the card in an available slot.

> **Note:** Some manufacturers suggest installing a driver prior to inserting the adapter card. It is therefore important to read the manufacturer's instructions before installing the card.

   a. Locate an open slot.
   b. Remove the slot cover.
   c. Firmly press the card into the slot.

> **Caution:** Do not rock the card side to side when installing or removing it.

   d. Secure the card to the chassis with the screw from the slot cover. Normally, you would now secure the cover back on to the system, but because you will be doing more work inside the system, leave it off.
3. Configure the card for the computer.
   a. Reconnect the peripherals and cables that you disconnected in step 1.
   b. Power on the system.
   c. Install any required drivers.
4. Check whether the card is functioning properly.
   a. Connect any devices to the card that are required for testing the card functionality.
   b. Access or use the device connected to the card.
   c. In **Device Manager,** verify that the device's properties show that the device is working properly and that there are no conflicts, and then select **Cancel.**

Topic D: Install and Configure Multimedia Devices

In the previous topic, you installed and configured expansion cards to support additional computer functionality. Once you have the right expansion cards in place, you can add peripheral components such as multimedia devices that provide users with additional and expanded capabilities such as recording music. In this topic, you will install multimedia devices.

As an A+ technician, you might support corporate users, such as marketing or sales representatives, who will need to create multimedia business presentations. Or, you might work for a retail computer outlet, supporting home users who like to play music and games on their PCs. Add to that the sheer number of multimedia devices that are now available for personal computer systems, and you will likely be tasked at some point with connecting and configuring a variety of multimedia devices for various types of end users.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.12: Install and configure various peripheral devices.

Multimedia Devices

A *multimedia device* is a computer peripheral or internal component that transfers sound, images or a combination of both to or from a personal computer. Multimedia devices can be input devices or output devices.

Figure: Multimedia devices.

Common Multimedia Devices

Common multimedia devices include different types of cameras and sound devices.

Multimedia Device	*Description*
Digital camera	A digital camera uses electronic signals to capture and store photographic images or video images. The resulting files are often stored on embedded memory cards, removable memory cards, or optical disks. Connecting the digital camera or its removable memory card to a PC enables you to save, transfer, print, and otherwise work with the images. If the digital camera has a removable memory card, the card itself may need to be connected to a computer through a media reader. Most digital cameras also offer USB and FireWire cables and connections.
Camcorder	A video recording camera captures and stores visual images and sounds in the form of either analog or digital signals. Video files are stored either on an internal storage device or on removable memory cards. Most digital camcorders available for personal (commercial) use also offer USB and FireWire cables and connections. If the camcorder has a removable memory card, the card itself may need to be connected to a computer through a media reader. Professional-grade cameras are more likely to use tapes or disks that will need an alternate transfer method, often including digitizing.
Webcam	A web camera, or webcam, is used to send periodic images or continuous frames to a website for display. Webcam software usually captures the images as JPEG or MPEG files and uploads them to a web server. Webcam images can also be accessed using some instant messaging software and by some video applications. Some corporations use webcams as a security measure. Webcams commonly use USB or FireWire cables and connectors.
MIDI-enabled device	The Musical Instrument Digital Interface (MIDI) connection enables you to connect and control musical devices such as electric keyboards, synthesizers, guitars, drum kits, and mixers. Sound cards usually include built-in synthesizers as well, to produce MIDI sounds. MIDI devices can be connected to each other and then to the computer. MIDI devices can connect to the computer using a number of ports. MIDI to USB interface, MIDI to serial, or MIDI to FireWire connections are most commonly used,

	allowing for faster communication between the musical instrument and the computer or controller device.
Microphone	A computer microphone is used to input audio into the device, either for recording the audio as data or for use in real-time, such as the audio input that accompanies a webcam or video conferencing chat. Microphones can be connected to the microphone port or jack of any sound card. If the card is color-coded, it will be pink. Otherwise, it will be labeled MIC or have a picture of a microphone. Many microphones have a 1/8-inch phono plug built into the attached cable.
Speakers	Speakers can be attached to the device to play the audio out loud, without the need for headphones. Speakers are connected to the line out port or jack on the sound card. Some speaker sets are permanently connected to each other. Other speaker sets are connected by the user to each other or to a subwoofer. A cable runs from one of the speakers to the line out port to connect both speakers to the computer. If the card is color-coded, the speaker port will be lime. The port might be labeled as Line Out, Out, Spkr, or Speaker, or it may have an image with an arrow indicating the direction of the audio (out). Speakers typically have a 1/8-inch phono plug built into the attached cable.

Line In

On many devices, there will be a third auxiliary port available: line in. Most PCs will have at least one line in jack, which provides a connection for a music player or other audio input device. If the sound card is color-coded, the line in port will be light blue. The port might be labeled as Line In or In, or it may have an image with an arrow indicating the direction of the input (in).

Note: Most desktop computers will have three auxiliary jacks available: microphone, line out, and line in. Most laptops don't have a line out or line in jack, but will typically have a microphone jack and a headphone jack.

Media Readers

A media reader functions as an interface between a removable memory card and a PC. Commonly connecting to the computer via a USB cable, a media reader is a small device that a user inserts a memory card into if that card does not have an interface of its own. For example, a Secure Digital (SD) card cannot be inserted directly into a computer, but by inserting the SD card into a media

reader and then connecting the media reader to the computer, the computer will recognize the SD card as another external storage device.

Multimedia Device Selection Tips

You will need to select a multimedia device that meets the user's needs and that can be supported on the user's machine. Depending on the multimedia device, there are a number of criteria to consider when making a selection.

Multimedia Device	***Considerations***
Digital camera	Determine what type of output the user needs from the camera. If the user plans to use the images only for viewing online, you can select a lower quality (fewer megapixels) camera. If the user also wants to print the images, particularly if the user wants large prints (such as 11-inch x 17-inch and higher), you should select a camera with as many megapixels as the user can afford. Keep in mind that you also need to have a means for the user to move photos off the device and onto the computer. Common techniques you can use include: • Connecting the camera directly to the computer via a USB or FireWire port. • Connecting the camera's memory card directly to the computer via a memory card slot. Not all computers have this feature, but many home PCs do. • Using a memory card reader that connects to a USB or FireWire port. Determine if you have the appropriate cables or connectors available that will be needed to connect the camera. Depending on the connector needed, make sure that there is also a port available on the device to connect the camera.
Camcorder	Determine what type of recording format/output the user needs from the camcorder. The format (analog or digital) can determine the cost of the device, the type and cost of any additional storage devices used with the device, how much video can be recorded, and the quality of the recordings and copies. Specifically, converting analog recordings to digital formats can be time consuming and usually results in degradation of quality. You should also consider the additional costs for the tapes or disks that will be used to record videos. which will vary depending on the manufacturer or type of device used. Determine if you have the appropriate cables or connectors available that may be needed to connect the camcorder. If the camcorder does not have external or removable storage, you may also need to have a solution for moving video files from the device and onto the computer, such as a FireWire cable. If a camcorder that records analog signals is being used, the user will likely need a digitizer (and the accompanying cables and connectors) to convert the files to digital

	format.
Webcam	Ensure that the user's computer has the necessary hardware, operating system, and memory required to support the device. Older computers may not meet the requirements. Different webcams offer different features: image quality can vary, lens quality and focus (manual versus automatic) can vary, they can be color or monochrome, some come with audio integrated and some need an external microphone. Determine what the user needs to do with the webcam and what features are indispensable. You will also need to determine if you have the appropriate cables or connectors available that may be needed to connect the webcam. You may also need to install an expansion card if the required port is not available on the computer. Many laptops will have a built-in webcam that is integrated into the system already.
MIDI-enabled device	Determine what kind of device is needed based on what the user needs or wants to do with the device. Once you know what kind of device they need, ensure that the user's computer has the necessary hardware and software to support the device. Determine if you have the appropriate cables or connectors available that may be needed to connect the device. You may also need to install an expansion card if the required port is not available on the computer.
Microphone	Users use microphones to complete tasks such as making phone calls through their computers and dictating to the computer using voice recognition software. For such users, the higher the quality of the microphone, the better they will be able to accomplish these tasks. Determine if you have the appropriate cables or connectors available that will be needed to connect the microphone. You will also need to make sure that there is an available port or jack available on the device to connect the microphone. Many laptops will have a built-in microphone that is integrated into the system already.
	If users plan to listen to music or play games on a computer, it is important to help them select higher-quality speakers. Key speaker standards include: • Stereo: Specifies a left and right speaker that connects directly to a single jack in a sound card. These types of speakers are usually the least expensive. • 2.1 Systems: Specifies a pair of stereo speakers plus a subwoofer. These systems

Speakers	do not support surround sound. • 5.1 Systems: Specifies five channels of sound: front-left, front-center, front-right, rear-left, and rear-right speakers, plus a subwoofer. • 7.1 Systems: Specifies seven channels of sound: front-left, front-center, front-right, middle-left, middle-right, rear-left, and rear-right speakers, plus a subwoofer. Determine if you have the appropriate cables or connectors available that will be needed to connect the speakers. You will also need to make sure that there is an available port or jack available on the device to connect the speakers.

Multimedia Device Installation Considerations

There are some considerations you should be aware of when installing multimedia devices.

Consideration	*Description*
Expansion card slots	If the device requires a specific expansion card, do you have an available slot on the motherboard? Also, try to place this expansion card in such a way as to avoid reducing the airflow in the computer.
Device drivers	Do you have the appropriate device drivers for the computer's operating system? If not, download them before starting the installation.
Cables and connectors	Do you have the necessary cables and connectors to connect devices, such as speakers, and place them where the user wants them?
Cameras and card readers	Although you can connect a digital camera directly to a computer to download its photos, you can use a memory card reader instead. The user will also see faster download performance when downloading photos using a memory card reader.

Note: Read the installation instructions for the device to determine if any software is required prior to the installation. Failure to do so could cause the installation to fail or the device and system to behave erratically.

LearnTO: For additional information, check out LearnTO **Install Multimedia Devices** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Multimedia Device Configuration

You can use multimedia device-specific software and either the **Device Manager** or the appropriate utility in the **Control Panel** to configure multimedia devices. Options you can configure for these devices include:

- Enabling and disabling a device.
- Selecting a default device for performing certain tasks, such as audio playback.
- Viewing and configuring features and properties for specific devices.
- Updating the device's driver.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Multimedia Devices**

ACTIVITY 3-8: Examining Multimedia Devices

Scenario

In this activity, you will examine multimedia devices.

1. **If you want to watch TV on your PC, but you do not need to record the transmission on your hard drive, which multimedia adapter should you use?**

   _x_ TV tuner card
   __ Capture card
   __ Video card
   __ NIC

2. **True or False? When you are installing a sound card, you do not have to worry about the available slots on the motherboard.**

   __ True
   _x_ False

ACTIVITY 3-9: Installing Multimedia Devices

Before You Begin

If your computer does not have integrated (onboard) sound support, a sound card has been installed. You have speakers, a microphone, and possibly other MIDI devices available to install.

Scenario

A group in the marketing department is responsible for creating and presenting audio-visual presentations. These users have sound cards installed on their systems. They all have speakers and microphones connected to their sound cards. Some of them also have MIDI instruments and instruments that connect through an 8-inch stereo jack. The users have just received these sound devices and want to begin using them.

1. Connect the speakers to the computer.
    a. Determine if you need to connect the speakers to each other, and if so, connect them to each other.
    b. Locate the speaker jack on the computer and plug the speaker cable into the jack.
    c. Test the speakers to ensure they are working properly.
2. Connect a microphone to the MIC jack.
    a. Locate the MIC jack on the computer and connect the microphone to the MIC jack.
3. Test the microphone.
    a. To test the microphone, select **Start→Control Panel→Sound.**
    b. Select **Sound Recorder.**
    c. In the Sound Recorder window, select **Start Recording.**
    d. Speak a few words into the microphone.
    e. Select **Stop Recording.**
    f. Save the file as ***Test Audio***
    g. Browse to the folder where the audio file is saved.
    h. Open the **Test Audio** file.
4. If you have a MIDI device, connect the MIDI device through the USB-to-MIDI device or a MIDI expansion card. Locate the appropriate port and connect the MIDI adapter to the appropriate port.
    a. If necessary, connect MIDI cables to the MIDI adapter.
    b. Connect the MIDI cable to the MIDI instrument.
    c. If necessary, install drivers for the MIDI instrument.
    d. Test the MIDI device by playing a few notes to ensure that it is working properly.
5. If you have another external multimedia device, connect it to the Line In jack.
    a. Locate the line in jack and connect an 1/8-inch stereo jack from the device to the computer.
    b. Test the device to ensure that it is working properly.
6. Close **Sound Recorder**.

Summary

In this lesson, you installed and configured various types of peripheral computer components, including input and output devices and the expansion cards that may be necessary to connect them. As an IT professional, having the ability to successfully install and configure these components is an integral part of a your daily work life, as you will be expected to set up workstations or assist users in installing anything that they may need to perform their job duties effectively.

What types of peripheral components do you anticipate having to install and configure most often in your current job role?

Will there be any specialty input devices that you will need to install or configure at your workplace? How might this affect your day-to-day activities as an IT professional?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 4: Managing System Components

Lesson Time: 4 hours, 35 minutes

In the previous lesson, you worked with peripheral components such as display devices, input devices, expansion cards, and multimedia devices. As an A+ technician, you are not only responsible for the components outside the system unit, but all the internal components as well. On the job, you may be asked to connect peripheral components for a user, or you may be asked to swap out a motherboard. In this lesson, you will explore the components that reside within a computer system.

A large part of your time as an A+ technician will be helping users to install and configure new software and hardware components. Having the knowledge and skills to properly install and configure the internal system components is crucial because, in most cases, users will not have the knowledge or the experience to install the components themselves. It will be your professional responsibility to know the technical specifications for these components and how to manage them appropriately.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Topic A:
  - Objectives 1.2, 1.3
- Topic B:
  - Objectives 1.2, 1.6
- Topic C:
  - Objective 1.8
- Topic D:
  - Objective 1.3
- Topic E:
  - Objective 1.5
- Topic F:
  - Objective 1.1

Topic A: Motherboards

In this lesson, you will dive inside the computer system and take a closer look at the internal components that enable the computer to run successfully. In this topic, you will start by examining motherboards.

The most important system component in a computer system is the motherboard. Although you can argue a case for almost any system component as being most important, without the motherboard, the computer simply cannot run. As an A+ technician, you must be knowledgeable about motherboards and their purpose within the computer system.

This topic covers all or part of the following CompTIA® A+® (2012) certification objectives:

- Exam 220–801: Objective 1.2: Differentiate between motherboard components, their purposes, and properties.
- Exam 220-801: Objective 1.3: Compare and contrast RAM types and features.

Motherboard Sizes/Form Factors

Motherboards come in several different sizes. This is often referred to as the board's *form factor*. The form factor describes the size, shape, and configuration of the motherboard.

System Board	***Form Factor***
ATX	ATX boards are an older motherboard standard that was introduced by Intel® in 1995 to provide better I/O support, lower cost, easier use, and better processor support than even earlier form factors. Some of the features of the ATX board are as follows: • Power supply with a single, keyed 20-pin connector. Rather than requiring Voltage Regulator Modules (VRMs) to reduce voltage down from 5 volts (V) to 3, 3 VDC is available directly from the power supply. • The central processing unit (CPU) is closer to the cooling fan on the power supply. Also, the cooling circulation blows air into the case instead of blowing air out of the case. • Input/output (I/O) ports are integrated into the board along with PS/2 connectors (instead of 5-pin DIN connectors). • You can access the entire motherboard without reaching around drives. This was accomplished by rotating the board 90 degrees. • This board cannot be used in Baby AT or LPX cases. • The board is 12 inches by 9.6 inches.
Mini-ATX	The mini-ATX board has a maximum size of 11.2 inches by 8.2 inches. The main difference between the mini board and the full-size ATX board is its smaller size. For example, it uses the same power supply form factor and case mounting holes as the full-size board.
microATX	The microATX board introduced in late 1997, is often written as µATX, and has a maximum size of 9.6 inches by 9.6 inches. MicroATX boards with integrated graphics are often used by system board manufacturers as a basis for small form factor and home entertainment PCs. MicroATX boards are backward compatible with the full size ATX boards and often use the same chipsets, so they can usually use the same components. However, because the cases are generally smaller, there are fewer I/O ports available than in ATX systems, so it might be necessary to use external USB hard drives, CD burners, and so forth.
	The mini-ITX motherboards are small, compact boards that fit the same form factor as the ATX and the micro-ATX boards. They have a maximum size of 6.7 inches by 6.6 inches.

mini-ITX	ITX boards were developed by a company named VIA technologies in 2001 to provide a compact board that does not drain system power. The boards are unique in that they are uniquely designed to consume less power while providing adequate processing power. Because of this, the board itself does not demand excessive cooling components. Due to their small size, and low power consumption, the boards can be implemented in a number of cases and electronics, and are popular among the industries that purchase motherboards in bulk to be incorporated into a number of different products.

Legacy System Boards

There are also a number of older model system board form factors that you might encounter on the job while supporting or repairing legacy systems. This information may be helpful to you in those situations and can be used as a reference.

System Board	***Form Factor***
Full-size AT	This form factor is usually used in older tower systems. Originally, it was designed from an even older system, the original XT motherboard, which itself was designed for use in the second version of the IBM® PC, released in 1983. These original full-size systems took up a large amount of desktop space. Vertically oriented tower systems using the AT board can stand on the floor and not take up desktop space, and they can still use the full-size system board. The board is 12 inches by 13.8 inches. A transfer bus of 16-bit or better is required. It uses complementary metal oxide semiconductors (CMOS) to retain configuration settings. It has a 5-pin DIN keyboard connection.
Baby AT	This form factor is usually used in older desktop systems. In an effort to free up desk space, manufacturers wanted to build a computer that was smaller than systems with full-size AT motherboards. The popular AT motherboard was scaled down to create the Baby AT motherboard. It fits into a smaller case than the full-size AT board, but it is otherwise the same. It works in any case except for those considered low profile or slimline. This was an extremely popular design. This board is usually 13 inches by 8.5 to 9 inches. It was never developed as a standard, so there are variations on the size of this particular board.
LPX	Slimline and low-profile cases, which are today's typical desktop cases, were being developed about the same time as the Baby AT motherboard was introduced. However, these smaller cases could not use even the Baby AT board. The LPX and Mini-LPX motherboards were developed for these cases. A riser card is used to plug expansion cards into the motherboard. This riser card enables the expansion cards to lie sideways, in the same orientation as the system board. Thus, the case does not have to be as high as the card. Another difference in this board is that it uses a PS/2-style keyboard connector rather than the 5-pin DIN connector used on the AT boards. Video, parallel, and two

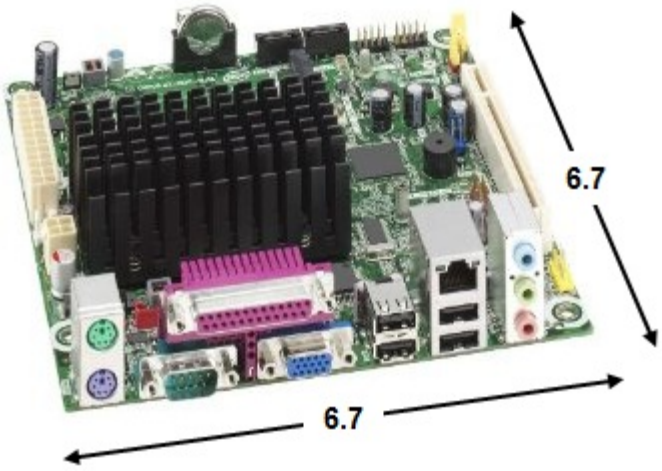
	serial ports were placed at the rear of the board in standard locations. This board is 9 inches by 11 to 13 inches. A mini-LPX board was also designed, which was 8 to 9 inches by 10 to 11 inches.
NLX	The NLX system board was developed to replace the LPX system board initially in 1997. It is a small form factor designed around the Pentium II processor. It supports advances in memory and graphics technology such as dual in-line memory modules (DIMMs) and accelerated graphics port (AGP). This board was designed to fix all the known issues with the LPX board and still fit slimline design systems. The board is 8 to 9 inches by 10 to 13.6 inches. The use of the NLX system board never really gained any headway with computer system manufacturers and was later replaced by the micro-ATX, FlexATX, and Mini-ITX boards.
BTX	Intended to be the replacement for the ATX system board form factor in 2005, the BTX form factor was designed to fix some of the issues that arose from using newer technologies (which often demand more power and create more heat) on system boards compliant with the circa-1996 ATX specification. BTX features include: • A low profile: The backplane is inches lower than the ATX. • Thermal design: The BTX layout establishes a straighter path of airflow with fewer obstacles, resulting in better overall cooling capabilities. • Structural design: The emerging need for heat sinks, capacitors, and other components dealing with electrical and thermal regulation has resulted in devices that can physically strain some motherboards. The BTX standard addressed this issue by specifying better locations for hardware mounting points. For example, the chips that make up the system's chipset are located closely to each other and to the hardware they control to reduce delays in data transfer. The BTX was discontinued by Intel in 2006.
MicroBTX (µBTX)	The MicroBTX is similar to the standard BTX system board, measuring 10.4 by 10.5 inches. The main difference between the standard board and the micro board is the smaller size and that the micro board has fewer expansion slots.
PicoBTX	The PicoBTX system board form factor is a smaller version of the standard BTX board measuring 10.5 inches by 8 inches. The pico board is designed with the same rear panels as the standard board and is used for half height or riser cards applications. Pico boards usually include only one or two expansion slots.

ACTIVITY 4-1: Identifying Motherboards

Scenario

In this activity, you will analyze and identify common motherboards in use today.

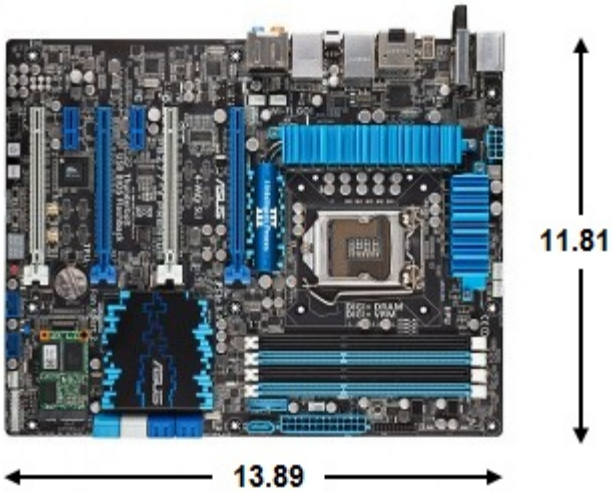
1. Examine the graphic and answer the following question.



What type of motherboard is displayed here, and what characteristics did you use to help you identify the board type?

A: Based on its small size dimensions and compact component design, this motherboard is a mini-ITX.

2. Examine the graphic and answer the following question.



What type of motherboard is displayed here, and what characteristics did you use to help

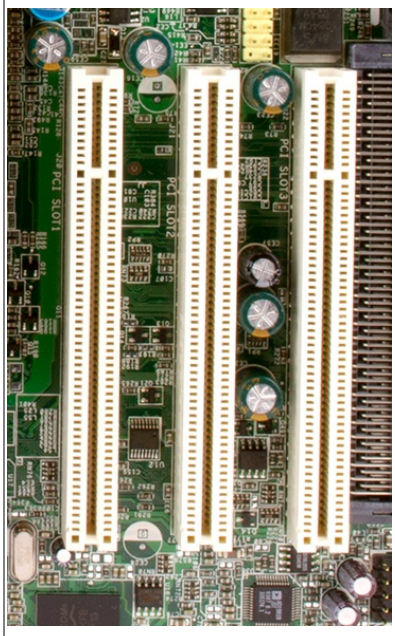
you identify the board type?

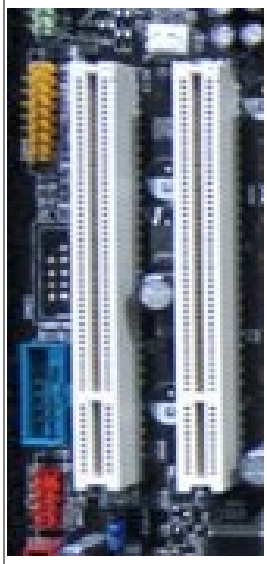
A: You can tell by the large size and vast number of available components and slots that this motherboard is an ATX.

3. Take the case off of the computer you are using for this course to identify the type of motherboard installed in the system. Use the descriptions presented in this topic to help you.

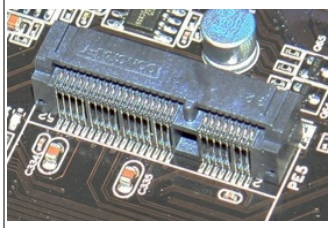
Expansion Slots

Expansion slots allow you to add expansion cards to your motherboard in order to extend the capabilities of a computer system. Motherboards generally include several of these slots so that the adapters can transfer data to and from the different computer components that have been installed in a system.

Expansion Slot Type	***Description***
PCI	The *Peripheral Component Interconnect (PCI)* expansion slot is the most common expansion slot used on system motherboards. The specifications include: • Physical characteristics of cards: 33 or 66 MHz. 133 MBps throughput at 33, 66, or 133 MHz. Up to eight functions can be integrated on one board. • Configuration: Supports up to five cards per bus and a system can have two PCI buses for a total of 10 devices per system. Can share interrupt requests (IRQs). Uses Plug and Play (PnP). • Used for all current adapters in client and server systems. • Number of data lines: 64-bit bus often implemented as a 32-bit bus. • Communication method: Local bus standard; 32-bit bus mastering. Each bus uses 10 loads. A load refers to the amount of power consumed by a device. The PCI chipset uses three loads, while integrated PCI controllers use one load. Controllers installed in a slot use 1.5 loads. 
	PCI-eXtended (PCI-X) is a motherboard expansion slot that improves upon some of the

PCI-X	PCI expansion capabilities and is the latest version of PCI technology. The specifications include: • Provides increased bandwidth and faster speeds by doubling the bus width from 32 bits to 64 bits. • Clock rate ranges from 66 megahertz (MHz) to 133 MHz, depending on the card. • Commonly found in server machines to provide faster transfer rates required. 

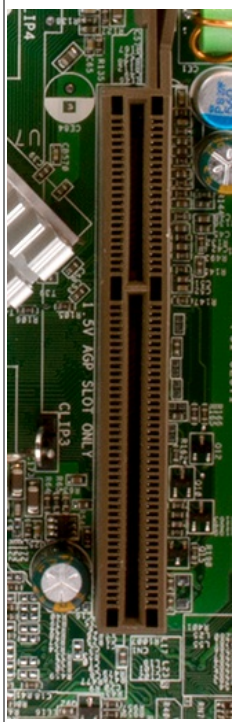
PCIe	The *PCI Express (PCIe)* slot and bus is an implementation of the PCI bus that uses a faster serial physical-layer communications protocol. It is the most common system bus found in PCs today. There are four versions of the PCIe standard—1.x, 2.x, 3.x, and 4.x. PCIe version 3.x is the current standard, which will eventually be replaced by version 4.x.
	• Used for high-speed graphics cards and high-speed network cards.
	• Number of data lines: Each device has a serial connection consisting of one or more lanes. The data rate depends on the PCIe version.
	  • PCIe version 1.x: Each lane offers up to 250 MBps of throughput. An x16 slot (16 lanes) can handle 4 GBps of bandwidth in one direction.
	  • PCIe version 2.x: Each lane offers up to 500 MBps of throughput. An x16 slot (16 lanes) can handle 8 GBps of bandwidth in one direction.
	  • PCIe version 3.x: Each lane offers up to 1 GBps of throughput. An x16 slot (16 lanes) can handle 16 GBps of bandwidth in one direction.
	  • PCIe version 4x: Specifications are not expected to be released until 2014,

	but the transfer rates are targeted to reach 16 gigatransfers per second (GT/s). • Communication method: Local serial interconnection.
MiniPCI	MiniPCI is a standard that was based on the PCI specification 2.2. It was specifically for use in laptops to implement a number of devices. The cards are attached to the motherboard and are not accessible from the outside of the laptop. There are three card form factors available: • Type I: Uses a 100-pin stacking connector • Type II: Uses a 100-pin stacking connector • Type III: Uses a 124-pin edge connector 
CNR	A Communications/Networking Riser (CNR) supports audio, modem, and local area network (LAN) functionality. • Physical characteristics of cards: Two rows of 30 pins, with two possible pin configurations. CNR Type A uses an 8-pin network interface, while Type B uses a 16-pin interface. Both types carry USB and audio signals. The slot is often brown and is usually located in the back-left corner of the system board. • Used for connecting audio, network, and modem cards, but is being phased out in favor of on-board components.

AGP

The *Accelerated Graphics Port (AGP)* bus was developed by Intel® specifically to support high-performance video requirements, especially fast 3D graphics.

- Physical characteristics of cards: Brown slot on the system board. AGP 1.0 is a 1x/2x slot. This is the shortest of the AGP slots with a small separator that divides it into two sections. AGP 2.0 is a 2x/4x slot that has extra pins at one end. There is also an AGP Pro slot. See **http://en.wikipedia.org/wiki/AGP** for more information.
- Have their own processors and cooling units attached.
- Used for video cards.
- Number of data lines: 32 bits wide with a throughput of 266 MBps for AGP 1x. Faster modes with throughput of 533 MBps are available on AGP 2x, 1.07 GBps for AGP 4x, and 2.1 GBps for AGP 8x.
- Communication method: Directly accesses Random Access Memory (RAM) rather than needing to transfer data to video RAM first.



ACTIVITY 4-2: Identifying Expansion Slots

Scenario

In this activity, you will examine and identify the expansion slots on your system's motherboard.

1. With the case removed from your computer, examine the expansion slots on your motherboard.
2. Try to identify the different types of expansion slots.

RAM Slots

RAM slots come in several form factors, and each module will connect to the system board through a RAM slot of a compatible type.

RAM Form Factor	***Description***
SIMM	Generally found in older systems, Single In-line Memory Modules (SIMMs) have a 32-bit data path. Because most processors now have a 64-bit bus width, they required that SIMMs be installed in matched pairs so that the processor could access the two SIMMs simultaneously. SIMMs generally have 8 memory chips per module. Only SIMMs can be installed into SIMM slots on the system board.
DIMM	Dual In-line Memory Modules (DIMMs) are found in many systems, and they have a 64-bit data path. The development of the DIMM solved the issue of having to install SIMMs in matched pairs. DIMMs also have separate electrical contacts on each side of the module, while the contacts on SIMMs on both sides are redundant. DIMMs generally have 16 or 32 chips per module.
SODIMM	Small Outline Dual In-line Memory Modules (SODIMMs) are half the size of DIMMs, and therefore cannot fit into a DIMM slot. SODIMMs are most often seen in laptops, small networking devices (such as routers), and PCs with smaller system boards. They have either 32- or 64-bit data paths.
RIMM	Rambus Inline Memory Modules (RIMMs) have a metal cover that acts as a heat sink. Although they have the same number of pins, RIMMs have different pin settings and are not interchangeable with DIMMs. RIMMs can be installed only in RIMM slots on a system board.

ACTIVITY 4-3: Identifying RAM Slots

Scenario

In this activity, you will examine and identify the RAM slots on your system's motherboard.

1. With the case removed from your computer, examine the available RAM slots on your motherboard.

2. **How many RAM slots are on your motherboard? Are they all being used?**

   A: Answers will vary depending on the individual computers.

Integrated I/O Port Types

System boards can include any or all of a number of integrated input/output controllers or ports: sound, video, network, modem, USB, serial, IEEE 1394/FireWire, parallel, and PS/2.

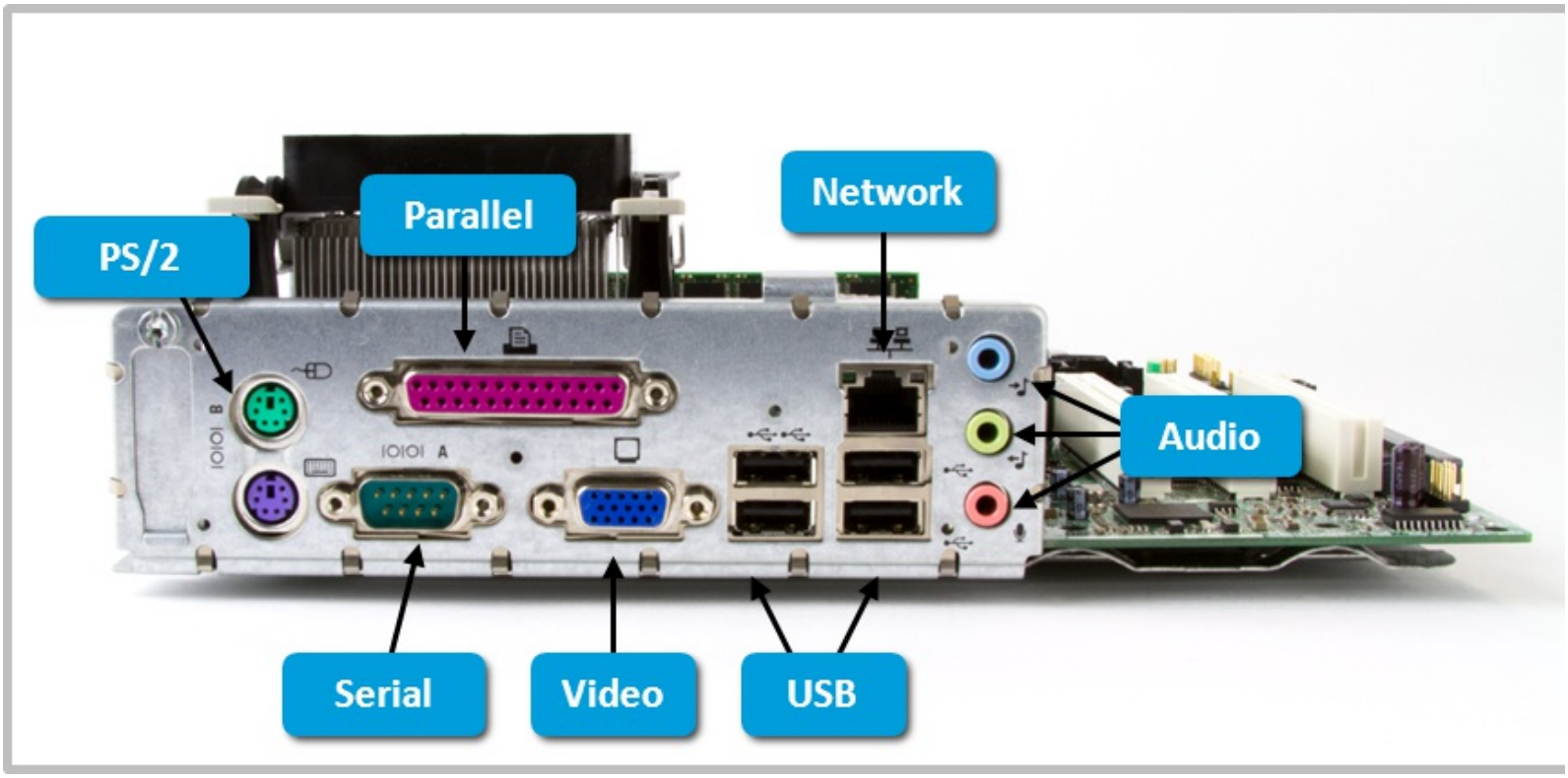


Figure: I/O ports on a motherboard.

Chipsets

The *chipset* is the collection of chips and integrated circuits that support basic functions of the computer. PC chipsets are housed on one to four chips and include built-in controllers for the system board's buses and all the integrated peripherals.

The chipset architecture, including the number, function, name, and placement of the various chips in a chipset, will vary depending on the type and manufacturer of the system board. For example, on many Intel Pentium computers, the two main chips in the chipset are known as the Northbridge and the Southbridge.

- The *Northbridge* controls the system memory and the AGP video ports, and it may also control cache memory. The Northbridge is closer to the processor and communicates directly with it using the system bus.

- The *Southbridge* controls input/output functions, the system clock, drives and buses, advanced power management (APM), and various other devices. The Southbridge is further from the CPU and uses the PCI bus to communicate with the Northbridge.

Newer Intel systems employ the Intel Hub Architecture (IHA) chipset. This also has two main chips, now named the Graphics and AGP Memory Controller Hub (GMCH) and the I/O Controller Hub (ICH), which perform functions roughly analogous to the Northbridge and Southbridge, but the communication between the two new chips is designed to be faster.

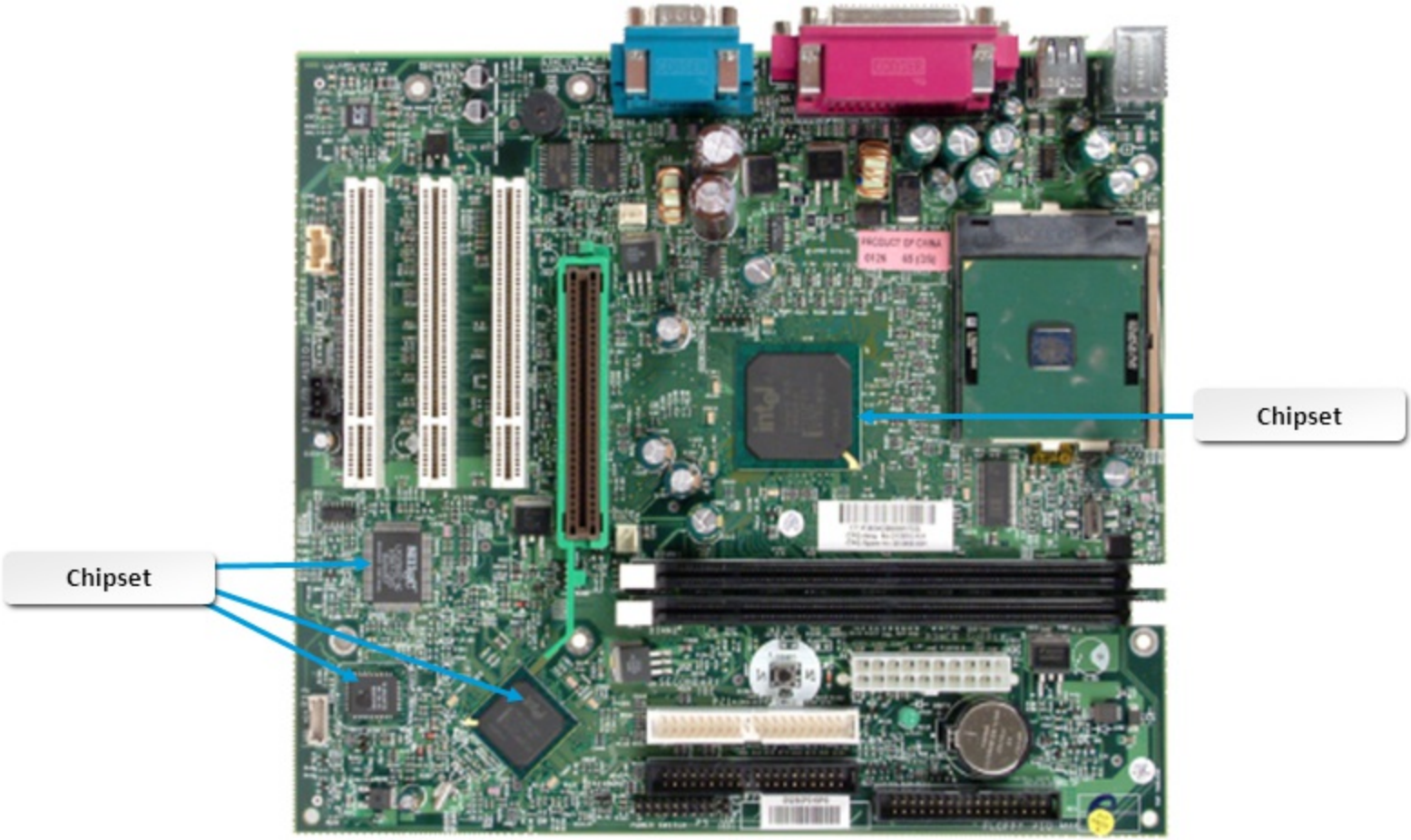


Figure: A chipset on a system board.

CMOS Battery

The *complementary metal-oxide-semiconductor (CMOS)* battery is a small battery on the motherboard that provides power to the real-time system clock when the computer is turned off. You may find cases when the CMOS battery fails, which will result in a CMOS Battery Failure message (or possibly a CMOS Read Error). Replacing a CMOS battery is not difficult, but it is not always necessary. Start by leaving the computer on for a day, and see if this helps the battery recharge. If this does not work, and you need to replace the battery, immediately write down all of your CMOS settings, as you will need to re-enter them later after replacing the battery. Note that not all motherboards can have their CMOS batteries replaced; in these cases you can add a new CMOS battery, but not remove the old one. Consult the documentation for your motherboard.

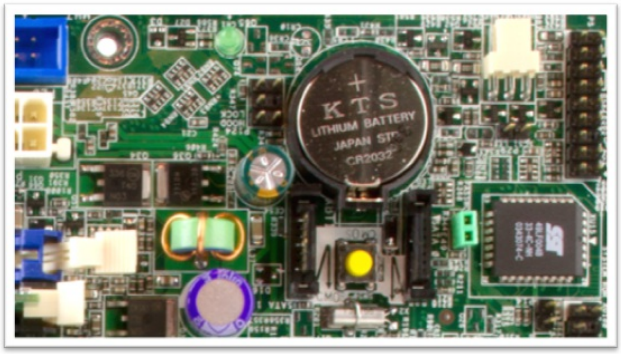


Figure: A CMOS battery.

CMOS Settings

CMOS settings can be changed if needed in the system setup program that is loaded from the BIOS setup utility. The CMOS battery supports the Basic Input/Output System (BIOS) utility by providing enough power to save critical system settings.

CMOS Setup Setting	***Description***
System date and time	You can set the system's real-time clock using DOS date and time commands, or by setting the clock in Windows, which will adjust the real-time clock.
Password	You can specify whether a user or administrator password is required to start up the system.
Boot sequence	You can specify the order that Power-On Self Test (POST) checks drives for an operating system.
Memory	Some systems require you to specify in CMOS how much RAM is installed on the system. You might also be able to specify whether the system uses parity memory or non-parity memory. Most modern systems automatically detect and report the installed RAM.

Hard drive	You can specify the number, type, and size of the hard drives attached to the system.
Floppy drive	You can adjust the speed and density settings for the floppy drive. You can also disable or enable a floppy drive.
Display	You can specify the monitor type and port.
Parallel/LPT ports	You can specify settings such as unidirectional or bidirectional printing, Enhanced Capability Port (ECP) options, and Enhanced Parallel Port (EPP) options. You can also disable or enable a parallel port. If you know that a parallel or serial port will not be used, you can disable the port, thereby freeing up the resources for use by other devices. Conversely, if you connect a device to a port and the device will not work at all, you might want to check the CMOS to ensure that the port has not been disabled.
Serial/COM ports	You can specify settings such as what memory addresses and interrupts are used by a port. You can also disable or enable a serial port.
Power management	In most modern computers, you can specify settings such as powering down components (such as the monitor, video card, and hard drives) when the components have not been used for a specified time period, as well as options and time limits for standby and suspend modes. You can also disable or enable global power management.

ACTIVITY 4-4: Identifying Other Motherboard Components

Scenario

In this activity, you will locate and identify various components on the motherboard of your system.

1. Look closely at the I/O ports on your system board and try to identify each one. You may need to look on the back of the system unit to identify all the ports.
2. On the motherboard, identify the chipset. How is it configured? Can you see the Northbridge and Southbridge chips? Or does this computer have the newer GMCH/ICH chipset?
3. Try to find the CMOS battery on the motherboard.

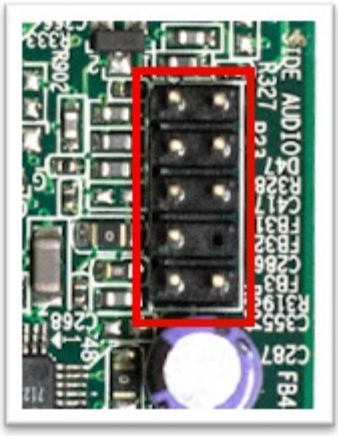
Jumpers and DIP Switches

Jumpers and dual in-line package switches (more commonly called *DIP switches*) are used to configure older system boards by shutting off an electrical circuit located on the motherboard. Using jumpers, this is accomplished by sliding a jumper shunt over the jumper pins on the *jumper block* of the motherboard. When using DIP switches, the numbered notches located on the switch can be moved to cut off the electrical circuit it is attached to. Newer motherboards are being designed to use software to configure these values (through the BIOS Setup program) instead of jumpers and DIP switches.

Front Panel Connectors

Many different components connect to the motherboard. It is important to understand where each component is supposed to be attached. Always check the manufacturer's information for your motherboard before you disconnect or reconnect a component to the pins on the various panels of the board.

Motherboard headers	***Description***
USB header	The USB header contains the pins that the USB cable connects to. This connects the USB drive installed in the computer case directly to the motherboard. USB headers will have one pin missing from the second row on the end. This can be a visual guide when identifying the different headers.
Front panel header	The front panel header of the motherboard contains many system connection pins that are used to connect components installed in the computer case to the motherboard. Most front panel headers will include: • Power switch • Power light emitting diode (LED) • Reset switch • Hard drive LED • Speaker

Audio header	The audio header contains the pins to connect the system audio cable to the motherboard. 

Fan Connectors

There are a number of uses for fans within a computer. The components installed and how much heat they produce will determine what type of fans are installed. Full size desktop systems will generally have a case fan that will pull the hot air out, letting the cooler air circulate through the chassis. There is no current standard that dictates the size and form factor of the fan connector. Common connectors include:

- A 3–pin Molex KK connector, commonly used to connect a fan directly to the motherboard.
- A 4–pin Molex KK connector is similar in function to the 3–pin KK connector, except that it has an extra pin to provide the ability to control the speed of the fan.
- A 4–pin Molex connector that connects directly to the system's power supply.

ACTIVITY 4-5: Identifying the Front Panel and Fan Connectors

Scenario

In this activity, you will identify the front panel connectors on the system board and any fan connections within the system unit.

1. On the motherboard, try to identify the front end connectors.
2. Check for any fans installed within the system. Locate the case fan and see how it is connected to the motherboard. Also check for any fans connected directly to the motherboard, and identify where the connections are made.

Bus Speeds

The motherboard bus speed determines how fast circuits will carry data simultaneously from one area of the motherboard to another. Speed can vary based on the capacity of the specific bus. The bus speed will depend on what components are installed in the computer.

Motherboard Power Connectors

The modern ATX power supply connection to the system board is a keyed connection that enables the power supply to provide power to the internal components of the system. Keyed connectors are designed so that the plug and socket have notches that must line up in order for the plug to fit into the socket. Older AT power supplies used two connectors, labeled P8 and P9. Be sure not to switch them when you plug them in or you could damage the system board. Most systems today have a single, keyed connector that can be inserted only one way, which prevents damage to the system board.

Power supplies have connections to other internal components as well. There are Berg and Molex connections, and older AT power supplies also had a connection to the power switch for the system.

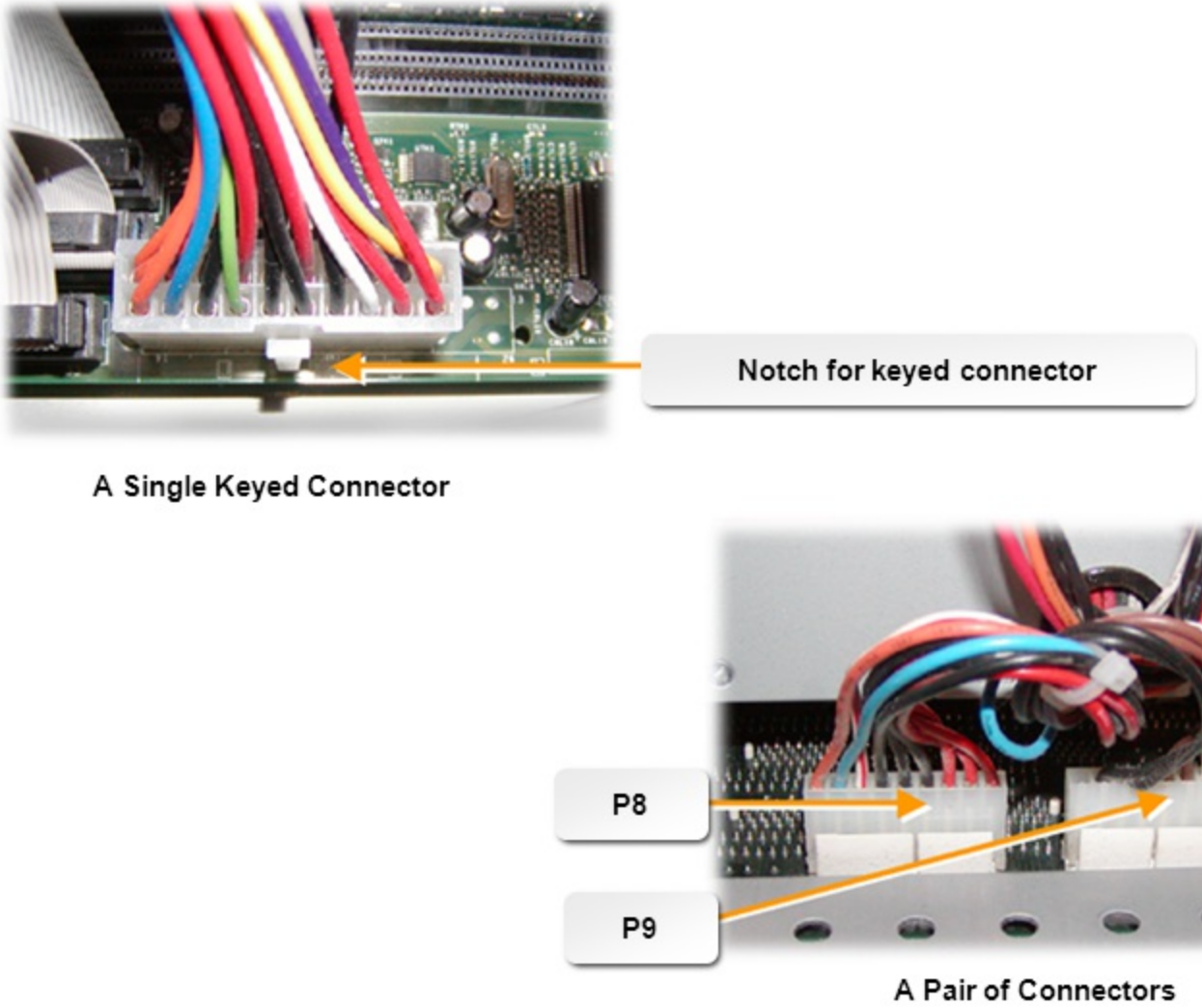


Figure: System board power supply connectors.

Specific Connectors

There are specific connectors, depending on the motherboard requirements, usually tied to the CPU type. There is the 20-pin (ATX), a 24-pin ATX connector, and the 20+4 combo (which you can

separate, or not, depending on the motherboard). This includes a 20-pin for the main power, plus a 4-pin connector for additional CPU power. This 4-pin is sometimes known as the Intel® Pentium® 4 connector. There is also an 8-pin CPU connector that requires an ATX 2.02 or an EPS12V PSU.

Motherboard Selection Tips

You will most likely select a motherboard based on what components you will need within the system. Use the table to help identify the system components you need and what impact that may have on the type of motherboard you choose.

System Component	***Questions To Ask***
Clock speed	Does the motherboard operate at a high enough frequency to support the processor you want to use?
CPU	What type of processor can you install? Can you install more than one CPU?
Drive interfaces	Does the motherboard include drive interfaces? If not, does it have enough available expansion slots to accommodate the user's hard disk requirements?
Expansion slots	How many expansion slots will the user need? What types of slots does it include? What type of expansion cards will you be installing?
Form factor	Will the motherboard fit inside the case of the computer?
Ports	Does the motherboard have the necessary ports to meet the user's needs? Specifically, does it have the parallel, serial, or multiple USB ports, and possibly FireWire ports needed?
RAM	Does the motherboard support enough Random Access Memory (RAM) to meet the user's needs?

Motherboard Installation Considerations

When you are replacing a motherboard, there are specific system requirements such as form factor, power needs, and component connections, that need to be considered. The process can be challenging based on a number of different requirements. The type of board you choose can also depend on the manufacturer's requirements for the system and you need to make sure you get one that fits your case. Cases will all have predetermined holes for the system board to line up to secure screws to the case.

Configuration and Optimization Requirements

When replacing and installing a new motherboard, you must ensure that it is properly configured to match the processor that it will host. In essence, you must configure the system board so that the internal and external frequencies of the processor are compatible. You can accomplish this by specifying a frequency multiple. Most system boards operate at a specific speed, but some enable you to select the speed via DIP switches, jumpers, or the BIOS setup software.

LearnTO: For additional information, check out LearnTO **Remove and Install Motherboards** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Motherboards**

Topic B: CPUs and Cooling Systems

In the last topic, you identified the various types of motherboards used in computer systems. Now that you understand the purpose of the motherboard, you can take a closer look at the components that make up the board. Two of these components are the central processing unit, or CPU, and the cooling systems that service it. In this topic, you will examine CPUs and cooling systems.

Much like the motherboard, the CPU is another important component of the computer system that actually carries out all the tasks requested by the applications installed in the computer. The CPU is a heat generator, so part of understanding the CPU includes understanding how to manage heat inside the computer case by managing the airflow and temperature. Keeping the system cool is an easy but important way to maintain or even increase its productivity. A computer that runs too hot risks damaging its own components. As an A+ technician, you need to be familiar with these essential components of the computer system.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.2: Differentiate between motherboard components, their purposes, and properties.
- Objective 1.6: Differentiate among various CPU types and features and select the appropriate cooling method.

CPU Sockets

CPUs use either sockets or slots to connect to the motherboard. Older slot-based processors plugged into a system board in much the same way as an expansion board, while socketed processors plug into a system board using a pin grid array (PGA). Modern CPUs usually fall into either the AMD or Intel category. While there are other CPU manufacturer brands available, Intel and AMD technologies tend to dominate in the marketplace.

Intel CPU Socket Types

While you may encounter older socket types on the job, most computers will use more recent socket types and processors. Common Intel CPU sockets include:

Socket Type	*Description*
LGA 775	The land grid array (LGA) 775 CPU is also referred to as Socket T. • Uses 775 copper pins with no socket holes to attach to the motherboard's pins. The CPU is connected via a load plate that the CPU attaches to and is lowered onto the board by a lever. • Proper cooling is accomplished by the design of the CPU connection to the motherboard. By using the load plate to connect, the CPU is properly seated into place and is perfectly level. This ensures that the CPU is making full contact with the heat sink or liquid cooling method. • Commonly used in consumer desktop computers. • Used for Pentium 4, Celeron D, Pentium Extreme Edition, Core 2 Duo, and Core 2 Extreme processors.
LGA 1156	The LGA 1156 is also referred to as Socket H or H1. • Uses 1,156 copper pins to attach to the processor pads on the motherboard. • Commonly used in consumer desktop computers. • Designed to replace the LGA 775 socket type. • Used for Core i3, Core i5, Core i7, Xeon, Celeron, and Pentium processors.
LGA 1155	The LGA 1155 is also referred to as Socket H2. • Uses 1,155 copper pins to attach to the processor pads on the motherboard. • Designed to replace the LGA 1156 socket type. • Used for Intel's Sandy Bridge and Ivy Bridge microprocessors.
LGA 1366	The LGA 1366 is also referred to as Socket B. • Uses 1,366 copper pins that connect to the bottom of the processor. • Commonly used in higher-end desktop systems that require high performance.

	• Used for Intel's X58 processor.
LGA 2011	The LGA 2011 is also referred to as Socket R, and was designed to replace LGA 1366. • Uses 2,011 copper pins that connect to bottom of the processor. • Commonly used in higher-end desktop computers and servers. • Used for Intel's Sandy Bridge and Ivy Bridge microprocessors.

AMD CPU Socket Types

Similarly to the Intel socket types, there will be, on occasion, an older socket and processor used, but in more cases, you will be supporting computers that contain newer-model AMD sockets and processors.

Socket Type	***Description***
940	The 940 was designed primarily for use in 64–bit server machines. Commonly found used with the Opteron and Athlon 64 FX processors.
AM2	The AM2 is similar to the 940 in design with the exception that it uses a DDR2 controller, instead of DDR used by the 940. This socket replaces the older Socket 939 and 754. This socket is commonly used with Athlon 64, Sempron, Athlon 64 X2 and Athlon 64 FX.
AM2+	The AM2+ was designed to replace the AM2. They are similar in design and are, in some cases, interoperable with the processors they support.
AM3	The AM3 was designed to replace AM2+. The socket is not compatible with the previous versions AM2 and AM2+ because of the pin layout being slightly different than the older models. The AM3 has 941 pins, while the AM2+ has 940.
AM3+	The AM3+, also referred to as AM3b, is designed to be more efficient and use less power.
FM1	FMI is AMD's next generation socket type that is designed to be used with the Fusion and Athlon II processors.
F	An older model socket type that was designed specifically for the Operton and Athlon 64 FX processors that used the LGA connection method.

Cache

Cache memory, or CPU cache, is a type of memory that services the CPU. It is faster than the main memory, is physically located closer to the processor, and allows the CPU to execute instructions and read and write data at a higher speed. Instructions and data are transferred from the main memory to the cache in blocks to enhance performance. Cache memory is typically static RAM (SRAM) and is identified by level. Level 1 (L1) cache is built directly into the CPU chip. Level 2 cache (L2) feeds the L1 cache. L2 can be built into the CPU chip, reside on a separate chip, or be a separate bank of chips on the system board. If L2 is built into the CPU, then a level 3 cache (L3) may also be present on the system board.

CPU Cache Types

There are three main types of cache found in modern computer systems:

- Instruction cache, which is used to retrieve and execute instructions faster.
- Data cache, which is used quickly retrieve and store data.
- Translation lookaside buffer (TLB), which is used to provide faster address translation for both data and instruction cache.

CPU Operational Characteristics

There are many different characteristics and technologies that can affect a CPU's performance.

CPU Characteristic or Technology	***Description***
Architecture	The CPU architecture is a description of the width of its front-side bus. A CPU's front-side bus width is either 32 or 64 bits.
Clock speed	The number of processing cycles that a microprocessor can perform in a given second. Some CPUs require several cycles to assemble and perform a single instruction, whereas others require fewer cycles. The clock speed is a technical rating; actual performance speeds can vary from the published clock speed rating. The clock speed is typically referred to as the processor performance.
Overclocking	Overclocking is configuring your system board to run at a speed greater than your CPU is rated to handle. Doing so can cause the CPU to overheat, produce random results, or be damaged or destroyed.
CPU speed	CPU speed is an umbrella term for the overall rate at which instructions are processed. There are two factors that affect the CPU speed. One is the core clock speed, which is the internal speed at which instructions are processed within the CPU. The other is the bus clock speed, which is the actual speed at which instructions are transferred to the system board.
Throttling	Used to adjust CPU speed. A CPU throttle is typically used to slow down the machine during idle times to conserve the battery or to keep the system running at a lower performance level when hardware problems have been encountered.
Hyperthreading (HT)	A feature of certain Intel chips that makes one physical CPU appear as two logical CPUs. It uses additional registers to overlap two instruction streams to increase the CPU's performance by about 30 percent.
Integrated GPU	The graphics processing unit (GPU) is integrated within the die of the CPU to provide an alternative to having a dedicated graphics card.
Virtualization support	Most modern CPUs are virtualization compatible, meaning that they have virtualization software built into the chipset of the CPU. Both Intel and AMD have CPU virtualization built into their chips. This allows the CPU to process instructions from multiple operating systems quickly and efficiently.
Cores	CPU cores read and execute instruction data sent from computer applications. A single chip that contains two or more distinct CPU cores that process simultaneously is called a multi-core. Options include dual-core (two CPUs), triple-core (three CPUs) and quad-core (four CPUs), though octo-core chips are becoming more common. Once you start adding tens or hundreds of CPUs, the terminology changes from "multi-core" and becomes "many-core."
Cache	Dedicated high-speed memory for storing recently used instructions and data.
VRM	A voltage regulator module (VRM) is a replaceable module used to regulate the

	voltage fed to the CPU.
MMX	Multimedia Extensions (MMX) is a set of additional instructions, called microcode, to support sound, video, and graphics multimedia functions.

CPU Selection Factors

Selecting a CPU for a computer can be a complicated process. Consider the factors provided to help you identify the requirements for both the CPU and motherboard.

Factor	*Considerations*
Compatibility	Start by checking the motherboard within the computer system. The design of the computer's motherboard determines the type of CPU you can install. For example, you cannot install an AMD processor into a system board designed to support an Intel processor. You should review the documentation for the computer's system board to determine its compatibility with other CPUs. Keep in mind that most original equipment manufacturers (OEMs) do not typically provide you with the system board's documentation. To obtain this documentation, try contacting the computer's manufacturer or the manufacturer of the system board. You can typically identify the manufacturer of the system board by examining it. It is critical that the motherboard is configured to properly support the new CPU. Most importantly, you might need to configure the system board to use the correct voltage. This is done by using the jumper settings on the system board or the computer's CMOS setup program. Setting the voltage on the system board too high can destroy the CPU.
Performance	In addition, you should keep in mind that there is a trade-off between price and performance when selecting a CPU. The greater the performance requirements of the user, the more powerful CPU you should select. And more powerful CPUs are simply more expensive. When selecting a CPU for a user, you should ask the user his budget for the purchase. This budget can help you narrow down the choices for selecting a processor.

Cooling System Types

Having the right cooling method can be crucial to reach the optimal performance of the system's CPU. Many cooling systems will be directly attached to the CPU.

Cooling System	***Description***
Fans	Computer fans provide cooling by simply blowing regular air across heated components. It is common to see case fans, power supply fans, adapter card fans, and CPU fans.
Vents	Computer cases are designed with vents to facilitate airflow through the case and across all components. A common implementation is to include air vents near the bottom of the front of the case and to place a fan near the top of the rear of the case to pull cooler air through the system.
Heat sinks	A heat sink is designed to provide direct cooling to a system's CPU. Modern CPUs have enormous processing power that requires instant cooling that is attached right the CPU itself. Heat sinks have metal fins to increase their surface area to aid in heat dissipation. Cool air is blown past it by a fan, removing the heat from the processor.
Thermal paste	Thermal paste is used to connect a heat sink to a CPU. At the microscopic level, when two solids touch, there are actually air gaps between them that act as insulation; the liquid thermally conductive compound gel fills these gaps to permit a more efficient transference of heat from the processor to the heat sink.
Liquid-based	CPUs can also be kept cool using a device to circulate a liquid or liquefied gas, such as water or freon, past the CPU. Like an air conditioner, heat from the CPU is absorbed by the cooler liquid, and then the heated liquid is circulated away from the CPU so it can disperse the heat into the air outside the computer. Liquid cooling systems are not as prevalent as heat sinks in most desktop systems or low-end servers.

Cooling System Selection Factors

When selecting a cooling system for a computer you must make sure that the following factors have been considered:

- What components need to be cooled?
- Will the cooling system fit within the computer case? Cooling systems come integrated within the computer case, while some can be installed externally.
- Do you need multiple cooling methods? Decide if you will need more than one cooling method installed. Most CPUs will have their own cooling system attached, so if you are in need of additional cooling, you should verify that a proper case fan is used as well.
- What size fan should be installed? The larger the fan, the more cooling power provided, so check what the maximum size fan opening is within your computer case before choosing the fan.

Computer Cases and Cooling

Although it might seem to be a good idea to remove the chassis cover to provide additional cooling, it is not recommended. Most PC cases have been designed to provide an airflow path, with fans positioned to keep the air moving and blow hot air away from heat-sensitive components. The PC case must be closed for this airflow path to work properly. If the case cover is removed, the fans will be less efficient, blowing air around at random.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure CPUs and Cooling Systems**

ACTIVITY 4-6: Selecting Cooling Systems

Scenario

In this activity, you will select cooling systems.

Selecting Cooling Systems

1. **When might you need more than one cooling system in a computer?**

   A: Answers will vary, but should include instances such as high processing levels that generate excessive heat.

2. **When would liquid cooling systems be more appropriate than adding a fan?**

   A: Answers will vary, but might include when there is not much room inside the computer case or when an externally mounted fan is not appropriate.

Topic C: Select and Install Power Supplies

In the previous topic, you examined CPUs and cooling systems. The next logical step is to select and install the power supply in the system unit. In this topic, you will take a closer look at the computer's power supply and its connections to the other system components.

The computer's power supply is the main source of power for all components installed within the system unit. Understanding the power requirements of all the components and the maximum power supplied is crucial in managing the overall computer system power needs. Whether you are upgrading or replacing faulty components, you need to effectively manage the capacity of the current power supply.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.8: Install an appropriate power supply based on a given scenario.

Power Supply Specifications

Each component in a personal computer has different power requirements that are required from the power supply. The specification provided will help in determining the right levels of power supplied to all internal computer components.

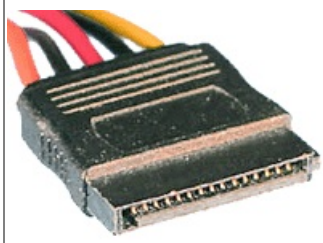
Specification	*Description*
Size	Hardware manufacturers across the globe strive to standardize the power supply unit specifications in terms of dimensions and layout to make computer users' lives simpler. This has resulted in a range of power supply unit types that are accepted worldwide. The key to replacing and installing a power supply is to make sure that the form factor matches the case and the motherboard it will connect to. Form factors available today are: • AT, which is used in AT form factor cases and with AT or Baby AT system boards. Dimensions are 213 mm x 150 mm x 150 mm. It is a legacy form factor found in older desktops and towers. • ATX, which can be used in ATX and NLX cases and with ATX and NLX motherboards. Dimensions are 150 mm x 140 mm x 86 mm. Found in desktops and towers. ATX power supplies do not have a pass-through outlet, but instead usually have a physical on-off switch. • Micro ATX is essential the same form factor as standard ATX, only with smaller wattage and physical size. • Proprietary, which include motherboards that do not conform to standards. It is likely that these proprietary system boards will require nonstandard power supply form factors as well, although you might be able to use an ATX power supply.
Connector styles	There are generally three types of connectors used to connect different devices in a computer to the power supply: • Berg, a square shaped connector used to supply power to floppy disk drives and some tape drives. • Molex, a round shaped connector used to supply power to Parallel ATA drives, optical drives, and SCSI drives. • SATA, used to supply power to Serial ATA drives.
	Power supply specifications are given in watts. Watts are volts times amps (voltage x current). Older systems typically had power supplies under 200 watts (W) and often even under 100 W. Newer power supplies typically have wattages ranging

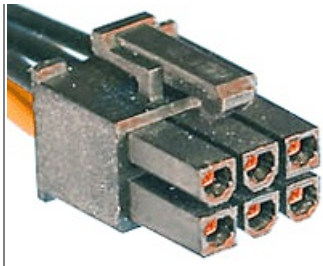
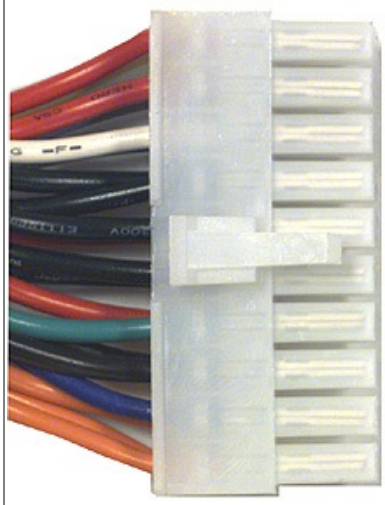
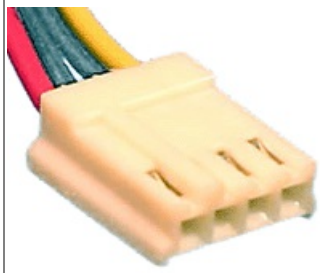
Wattage	from 200 to 500 W. Because of their increased power demands, high-powered servers or computers designed for gaming can have power supplies with wattages from 500 W up to 1 kilowatt (kW).
Voltage	All system components require specific voltages. Some devices have different voltage requirements depending on use. This is particularly true of some memory chips, which vary in voltage requirements from 1.8 volts (V) to 3.3 V, and some can actually function at different voltages (voltage range). You must verify that the power supply used can provide the volts demanded by the system. Some power supplies are dual-voltage power supplies. They can contain multiple channels that provide discrete voltages, with 5 V, 12 V, 15 V, and 24 V being the most common. In order to calculate whether your power supply meets your power needs, you will need to add up the maximum power you might use at one time. A range of maximum power consumption for various components has been established. Most components use much less than the maximum, so by using the published requirements as a guide, you are overestimating the power usage, and therefore making it more likely that you never test the capacity of the power supply. You can check the documentation for the component to determine how much power it actually will use. Even some of the most powerful current CPUs, such as the Intel Core 2 Extreme and the AMD Opteron Dual Core, only use 1.1 to 1.3 V. The necessary voltage for CPU and RAM is usually detected by the motherboard (BIOS) and configured appropriately, but sometimes you have to manually configure it by accessing the BIOS and entering the appropriate values. The power supply will supply 3.3 V for the CPU, RAM, and other devices, but the motherboard regulates how much they actually get.

Note: Although most devices require specific voltages, some devices have different voltage requirements depending on use. This is particularly true of some memory chips, which vary in voltage requirements from 1.8 V to 3.3 V, and some can actually function at different voltages, or in a voltage range.

Power Supply Connections

One of the first things you will notice about a power supply is the cable that connects it to the components within a computer because there are so many different colored wires and connectors. Every device uses one of several types of connectors to connect to the computer's power supply.

Connector Type	***Description***
SATA	The 15-pin Serial Advanced Technology Attachment (SATA) connector connects peripheral components to the power supply and has a maximum wattage of 54. The SATA connector provides power at three voltages: • +3.3 • +5 • +12 
4/8–pin 12 V	The 4-pin and 8-pin connectors are similar in that they both provide 12 volts of power to the CPU on the motherboard. The 8-pin was designed to provide power to multiple CPUs in the system. The 4-pin has a maximum wattage of 192, and the 8-pin has a maximum wattage of 336.
PCIe 6/8–	The Peripheral Component Interconnect Express (PCIe) 6-pin and 8-pin connectors provide power to PCIe slots on the motherboard. Both connectors provide power at 12 V. The 6-pin has a maximum wattage of 75, while the 8-pin has a maximum wattage of 150.

pin	
Main power connectors	The main power connector to the motherboard is either a 20-pin or 24-pin ATX connector. The 24-pin connector contains four additional pins to support the requirements for PCI Express slots on the motherboard. The 20-pin connector has a maximum wattage of 72, while the 24-pin has 144. Both connectors provide power at three voltages: • +3.3 • +5 • +12 
Floppy	The floppy connector is a Berg connector and was used to connect floppy drives to the power supply. The connector has only four pins and provides power at +5 and +12 V with a maximum wattage of 36. 

ACTIVITY 4-7: Identifying Power Supply Connections

Scenario

In this activity, you will identify the various power supply connections within your system.

Identifying Power Supply Connections

1. Locate the power supply within your system.
2. Trace the connections from the power supply to the motherboard and identify the type of connections made.

Power Supply Safety Recommendations

Power supplies can be very dangerous to work with. You should take careful security measures when working with power supplies.

Safety Precaution	*Explanation*
Check for certification	Be sure to purchase power supplies that are certified by the Underwriters Laboratories, Inc. (UL). UL standard #1950, the "Standard for Safety of Information Technology Equipment, Including Electrical Business Equipment, Third Edition," regulates computer power supplies (along with other components). When it comes to electricity, you do not want to take a chance with a non-certified power supply. The risk of electrocution or fire from a malfunctioning power supply is simply not worth saving a few dollars by purchasing a low-quality power supply.
Replace instead of repair the power supply	You run the risk of electrocution if you open a power supply to attempt to repair it. Even when you unplug a computer, the power supply can retain dangerous voltage that you must discharge before servicing it. Because power supplies are relatively inexpensive, it is easier (and safer) to simply replace a failed power supply rather than attempting to repair it.
Keep the computer case on	Make sure that you run computers with their cases on. The fans inside power supplies are designed to draw air through the computer. When you remove the cover, these fans simply cool the power supplies and not the computer's components. Leaving the case open puts the computer at risk of overheating.
Protect the power supply	Use a power protection system such as an uninterruptible power supply (UPS) or surge suppressor to protect each computer's power supply (and thus the computer) from power failures, brownouts, surges, and spikes. You should also make sure that the computer's power cord is plugged into a properly grounded electrical outlet. (Three-pronged outlets include grounding; never use an adapter to plug a computer's power cord into a two-pronged electrical outlet.) You can buy a socket tester (available at hardware stores) to test your outlets if you suspect that they are not properly grounded.

Note: You should also make sure to cover empty slots in the system board with filler brackets. If you do not install a filler bracket, you reduce the efficiency of the power supply's fan and increase the chances of the computer overheating.

Selecting the Right Power Supply

Selecting the right power supply can be overwhelming, as effective performance depends on all of the components you plan on installing in the system. If you are building a computer from scratch, then selecting a power supply is a bit more tedious than just installing a replacement that meets the manufacturer's requirements. Each system component has its own power needs and requirements, so selecting the right power supply will enable all these components to function properly. Things you should consider include the total system requirements for power, the form factor for the unit, and whether there is adequate cooling within the system. When determining the cooling requirements, some power supplies can be examined to see the revolutions per minute (RPMs) of the power supply fan. You can then adjust the fan speed to run at only the speed needed to cool your system. This can reduce power consumption and save fan wear and tear.

LearnTO: For additional information, check out LearnTO **Install a Power Supply** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Select and Install Power Supplies**

ACTIVITY 4-8: Calculating Power Requirements

Scenario

In this activity, you will calculate the power required by the computer you are using for this course. As a guide, you can refer to the following table that includes common component types and example specifications and required wattages.

Component Type	*Example Specification*	*Example Wattage Required*
CPU	Intel Core i7-970, 3.2 GHz	130
Memory	4GB DDR3-1600	8
Video card	NVIDIA GeForce 8800 GTS	220
Motherboard	ASUS P6X58D Premium LGA	36
Hard drive	1 TB SATAII 7200 RPM	6
Optical drive	6x Blu-ray	32
NIC	10/100/1000 Mbps PCI-Express	14
Sound card	SoundBlaster X-Fi Titanium	23
USB wired keyboard	Yes/No	4
USB wired mouse	Yes/No	4
USB flash drive	Yes/No	5
Other external devices	External DVD+R drive	External DVD+R drive: 5

1. Examine your computer, and complete the **Specifications** row of the table in step 2. If you have different or additional components in your PC, revise the table accordingly.
2. Determine the power required by each component, and complete the following table. Again, example values have been provided for your reference.

Component Type	*Specification*	*Wattage Required*
CPU		
Memory		
Video card		
Motherboard		
Hard drive		
Optical drive		
NIC		
Sound card		
USB wired keyboard		
USB wired mouse		
USB flash drive		
Other external devices		

3. Calculate the total wattage required for your system. Compare this value with the maximum wattage output listed on the power supply. Does this power supply need to be upgraded?
4. Add a buffer of 30 percent to the total wattage required for your system. Will the existing power supply continue to supply enough power if additional components are added to the system?

ACTIVITY 4-9: Replacing a Power Supply

Scenario

After calculating the power needed for all the components added to a user's system, you have determined that it exceeds the capacity of the installed power supply. You have ordered and received a replacement power supply and now you need to install it.

Replacing a Power Supply

1. Remove the existing power supply.
    a. Shut down and turn off the system.
    b. Unplug the power cord from the electrical outlet.
    c. On AT systems, to discharge any remaining electricity stored in the computer's capacitors, toggle the power switch on the computer on and off.
    d. Remove any components necessary in order to access the power supply and its connection to the system board.
    e. Unplug all power connections from devices, marking where each connection went to as you go.
    f. Unplug the power supply from the system board.
    g. Unscrew the power supply from the case.
    h. Remove the power supply from the case.
2. Install the replacement power supply.
    a. Insert the power supply into the case. Align the guides on the base of the supply with the base.
    b. Secure the power supply to the case.
    c. Plug all power connections into the devices.
    d. Plug the power supply into the system board.
    e. Reinstall any components you removed to access the power supply.
    f. Plug the power cord from the power supply to the electrical outlet.
3. Test the power supply.
    a. Turn on the system.
    b. Test all components.

Topic D: RAM Types and Features

In the previous topic, you examined the requirements of the system's power supply. Providing sufficient electrical power is one way to ensure that system components run at an acceptable performance level, but it is not the only solution you should consider. In this topic, you will examine RAM.

Just as some people say you can never be too rich or too thin, you can never have too much memory. Adding memory is one of the simplest and most cost effective ways to increase a computer's performance, whether it is on a brand-new system loaded with high-performance applications or an older system that performs a few basic tasks. Upgrading the memory is a common task for any PC technician.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220-801 certification objectives:

- Objective 1.3: Compare and contrast RAM types and features.

RAM Modules

A *RAM module*, or *memory module*, is a printed circuit board that holds a group of memory chips that act as a single memory unit. Memory modules reside in slots on the motherboard, and they are removable and replaceable. Memory modules are defined by their design, and by the number and type of chips they contain.

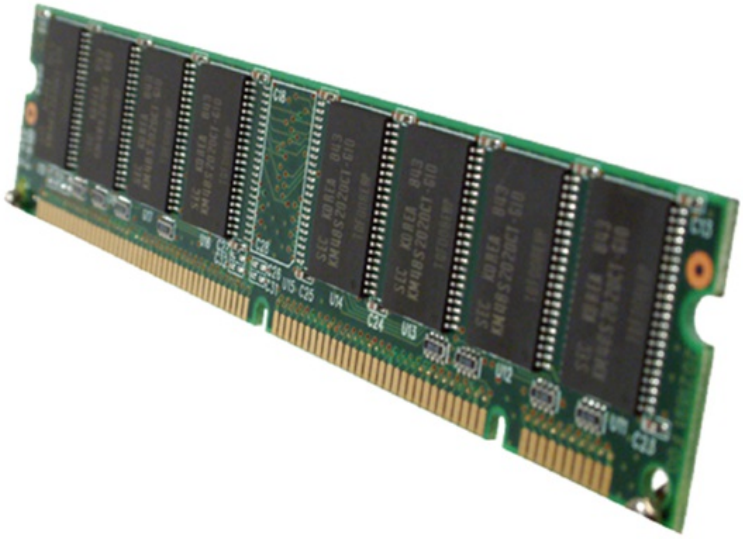


Figure: A memory module.

Single-Sided vs. Double-Sided Memory

Single-sided RAM does not refer to the literal number of sides that a RAM module has, but rather it means an expansion bank of RAM has all of its available memory accessible by the computer. Double-sided RAM might have two banks of memory, but only one can be accessed at a time by the computer.

Note: Whether a RAM module has chips on one side or two, if the computer can access all of its memory at once, the RAM module is considered to be single-sided.

RAM Configurations

There are three different chipset configurations used in RAM that will determine how fast data can be transferred between the chips on the board. The slowest is the single channel because it is limited to only one channel for communication. On the other hand, double channel can transfer data twice as fast as single, because it has two channels in which to send and receive data. The fastest configuration is called triple channel, and it uses three channels for data transfer and is three times as fast as single channel.

Intel has recently introduced a fourth RAM configuration that can support a quadruple channel architecture, but there are restrictions based on the limitations from system components within the system.

Types of RAM

There are several types of RAM.

Type of RAM	*Description*
SRAM	Static RAM (SRAM) is used for cache memory, which is high-speed memory that is directly accessible by the CPU. It does not need to be refreshed to retain information. It does not use assigned memory addresses. It is faster than Dynamic RAM, but it is also more expensive.
DRAM	Dynamic RAM (DRAM) is used on single and dual in-line memory modules (SIMMs and DIMMs). It is the most common type of RAM. It needs to be refreshed every few milliseconds. It uses assigned memory addresses and can be implemented using Synchronous DRAM, Direct Rambus DRAM, or Double Data Rate SDRAM.
DRDRAM	Direct Rambus DRAM (DRDRAM) is implemented on a RIMM memory module. It is a type of synchronous, dynamic RAM.
SDRAM	Synchronous DRAM (SDRAM) runs at high clock speeds and is synchronized with the CPU bus. SDRAM was originally packaged on a 168-pin DIMM.
DDR SDRAM	Double Data Rate SDRAM (DDR SDRAM) transfers data twice per clock cycle. It is a replacement for SDRAM. DDR uses additional power and ground lines and is packaged on a 184-pin DIMM module.
DDR2 SDRAM	DDR2 chips increase data rates over those of DDR chips. DDR2 modules require 240-pin DIMM slots. Although DDR2 chips are the same length as DDR, they will not fit into DDR slots.
DDR3 SDRAM	DDR3 chips transfer data at twice the rate of DDR2, and use 30 percent less power in the process, Like DDR2, DDR3 chips use 240-pin connections, but cannot be used interchangeably because of differences in notch location and electrical requirements.

Types of ROM

ROM is memory that is non-volatile. The original ROM chips could not be altered after the program code was placed on the ROM chip. As time went on, though, users needed the ability to update the information stored on ROM chips. Over the years, various chips have been created that perform the function of ROM, but can be updated one way or another. These are referred to as programmable ROM (PROM). Types of ROM include:

- PROM: A blank ROM chip that is burned with a special ROM burner. This chip can be changed only once. After the instructions are burned in, it cannot be updated or changed.
- EPROM (erasable PROM): Like PROM, except that the data can be erased through a quartz crystal on top of the chip. After removing the chip from the system, an ultraviolet (UV) light is used to change the binary data back to its original state, all ones.
- EEPROM (electronically erasable PROM): A chip that can be reprogrammed using software

from the BIOS or chip manufacturer using a process called flashing. Also known as Flash ROM. The chip does not need to be removed in order to be reprogrammed.

Memory Standard Specifications

The following table summarizes the memory standard specifications.

Standard	*Characteristics*
PC100	• Clock speed: 100 megahertz (MHz) • Bus width: 8 bytes • Voltage: 3.3 V • Form factor: 168-pin DIMM and 144-pin SODIMM • Transfer rate: 763 MBps • Backwards-compatible with PC66
PC133	• Clock speed: 133 MHz • Bus width: 8 bytes • Voltage: 3.3 V • Form factor: 168-pin DIMM and 144-pin SODIMM • Transfer rate: 1,015 MBps • Backwards-compatible with PC100
DDR-333 or PC2700	• Clock speed: 166 MHz • Bus width: 8 bytes • Voltage: 2.5 V • Form factor: 184-pin DIMM • Transfer rate: 2,533 MBps • Backwards-compatible with slower DDR SDRAM DIMMs

DDR-400 or PC3200	• Clock speed: 200 MHz • Bus width: 8 bytes • Voltage: 2.6 V • Form factor: 184-pin DIMM • Transfer rate: 3,052 MBps • Backwards-compatible with slower DDR SDRAM DIMMs
DDR2–667, PC2-5300, or PC2-5400	• Clock speed: 166 MHz • Bus width: 8 bytes • Voltage: 1.8 V • Form factor: 240-pin DIMM • Transfer rate: 5,066 MBps • Backwards-compatible with slower DDR2 SDRAM DIMMs
DDR3–1600 or PC3-12800	• Clock speed: 200 MHz • Bus width: 8 bytes • Voltage: 1.5 V • Form factor: 240-pin DIMM • Transfer rate: 12,207 MBps

ECC

Error Correcting Code (ECC) is an error correction method that uses several bits in a data string for error checking. A special algorithm is used to detect and then correct any errors it finds. ECC is used only in upper-end systems such as high-end workstations and servers; other desktop systems use non-ECC memory. Non-ECC memory usually employs *parity* to ensure that errors are detected within the data, but does not have the functionality to correct them.

Parity

Parity is an error-checking method that is sometimes used in RAM modules to detect errors that may occur during data transmission. When parity is used, a data transmission contains 8 bits of data with the ninth bit being the parity bit. The parity bit is used to determine whether a piece of data is equal to another piece of data. The parity bit value can be either true, or a 1, or it can be false, or 0. An error is detected if the parity bit values of two data strings do no match. When an error is detected, the system simply tries again after discarding the data. Parity memory is rarely used; however, there are usually other system components that are relied on to verify that the data contained in memory is accurate when non-parity memory is used. You will typically find this type of memory used in servers.

RAM Characteristics

There are several factors you should consider when purchasing RAM for a computer.

RAM Characteristic	*Questions to Ask*
Compatibility	Is the RAM compatible with the system's motherboard? What is the maximum RAM size supported by the computer's motherboard? What channel architecture does the RAM support? What architecture is desired based on the requirements of the system's motherboard?
Speed	What is the current speed of the RAM in the computer? What is the bus speed of the computer? RAM speed is the time needed to read and recharge a memory cell, and is measured in nanoseconds (ns). A nanosecond is one-billionth of a second. The smaller the number, the faster the RAM. For example, 10 ns RAM is faster than 60 ns RAM. All of the RAM in the system runs at the lowest common speed. It is backward-compatible, so it can run at the lower speed if it finds slower RAM. Some systems will not run with mixed RAM speeds, but these are not common. Also, the RAM will not run any faster than the system board's bus speed.
System board configuration	Do you need to install RAM in pairs of memory modules? What is the size of the connector for RAM chips?

RAM Speed

Older Ferroelectric Random-Access Memory (FPRAM) was often 60- to 70-nanosecond (ns) speed RAM. Modern RAM that you are likely to find runs at clock speeds of 100 MHz and 133 MHz. The 100 MHz RAM has a RAM speed of 10 ns. The 133 MHz RAM has a RAM speed of 6 ns. The SDRAM used in 168-pin DIMMs has access times in the 6 to 12 ns range.

Determine and Upgrade Your RAM

If you wish to upgrade your computer's RAM, some vendors (such as Crucial: **www.crucial.com/index.aspx**) have a downloadable utility that scans your computer and tells you what kind of upgrade is compatible with your machine.

ACTIVITY 4-10: Comparing RAM Types and Features

Scenario

In order to choose the right type of RAM for a computer system, you typically will compare the various types and features.

1. **When selecting a new RAM module, how do you determine the maximum running speed of the RAM once it has been installed?**

   A: The RAM module can run only as fast as the motherboard's bus speed, so you must determine the maximum speed of the system bus.

2. **On a typical system with RAM that runs at 10 ns, what RAM can you add? (Select all that apply.)**

   _x_ RAM that runs at 10 ns
   _x_ RAM that runs at 12 ns
   _x_ RAM that runs at 6 ns
   _x_ RAM that runs at 8 ns

3. **When selecting a RAM module, when would you choose RAM enabled with ECC as opposed to RAM with only parity?**

   A: The difference between ECC and parity is that ECC can detect errors and correct them, while parity can only detect errors. If you are adding or replacing RAM in a high-end system or a server where errors can have a critical impact on data integrity, you should consider choosing ECC RAM.

Topic E: Install and Configure Storage Devices

In the previous topics, you identified a number of system components that you may have to install and configure on a computer system. Storage devices such as hard disks are one of the most common system components you will install. In this topic, you will install and configure storage devices.

Users rely on local storage devices to keep their applications and data current and available. As an A+ technician, your responsibilities are likely to include installing and configuring different types of storage devices to provide your users with the data-storage capabilities that they need to perform their jobs.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.5: Install and configure storage devices and use appropriate media.

Media Capacity

There are several media types available to users for storing their data. The capacity for any type of media will depend on what the capacity is. Each media type has a limit to the amount of data it can store.

Media	*Capacity*
CD/CD-RW	The capacity for CD-ROMs ranges from 700 to 860 MB.
DVD/DVD-RW	• Single-sided (single-layer): 4.7 GB • Single-sided (double-layer): 8.7 GB • Double-sided (single-layer): 9.4 GB • Double-sided (double-layer): 17.08
Blu-ray	Blu-ray discs have a capacity of up to 128 GB, depending on the number of layers. Each layer on the disc has a capacity of 25 GB. Newer discs have the capability of holding up to four layers of storage.
Tape	Tapes are generally used to backup data. Higher-end tapes can store up to 5 TB of digital data.
Floppy	Floppy disks are rarely used any longer. Regular 3.5 inch floppy disks had a capacity of 720 KB or 1.44 Mb. Super floppy disks are rarely used today and only have a capacity ranging from 100 to 200 MB.
DL DVD	Dual layer (DL) DVDs have a capacity of 8.5 GB.

Single- and Double-Sided Media

Single-sided and double-sided have two meanings when discussing computer memory, depending on the media type. Single-sided removable media refers to a disc (floppy, CD, or DVD) that can be read and written to one side only. Double-sided discs or DVDs can be read from and written to both sides, thus doubling the storage capacity of the media.

RAID Standards

The *Redundant Array of Independent Disks (RAID)* standards are a set of vendor-independent specifications for improvements in performance and/or fault-tolerant configurations on multiple-disk systems. In a fault-tolerant configuration, if one or more of the disks fails, data may be recovered from the remaining disks.

RAID can be implemented through operating system software, but hardware-based RAID implementations are more efficient and are more widely deployed. Hardware-based RAID requires a card, or controller, to show the different disks to the computer as a single drive. These cards are usually a PCI or PCIe card, but can also be already built into the motherboard. There are several RAID levels, each of which provides a different combination of features and efficiencies. RAID levels are identified by number; RAID 0, RAID 1, and RAID 5 are the most common.

Note: The original RAID specifications were titled Redundant Array of Inexpensive Disks. As the disk cost of RAID implementations has become less of a factor, the term "Independent" disks has been widely adopted instead.

Common RAID Types

RAID 0, 1, 5, and 10 are the most common implementations.

RAID Type	*Description*
RAID 0	RAID level 0 implements *striping*, which is the process of spreading data across multiple drives. Striping can dramatically improve read and write performance. Striping provides no fault tolerance, however; because the data is spread across multiple drives, if any one of the drives fails, you will lose all of your data. You must have at least two physical disk drives to implement striping, and the largest size RAID-0 partition that can be created is equal to the smallest available individual partition times the number of drives in the set. For instance, combining a 37 GB drive and a 100 MB drive in a RAID 0 set would result in a 200 MB partition; the balance of the 37 GB drive could not be included in the set (although it would remain available for use in other partitions).
RAID 1	In RAID level 1, data from an entire partition is duplicated on two identical drives by either mirroring or duplexing. In *mirroring*, the two disks share a drive controller. In *duplexing*, each disk has its own drive controller, so the controller card is not a single point of failure. Data is written to both halves of the mirror simultaneously. This redundancy provides fault tolerance and provides for quick failure recovery, but the storage overhead consumes half the available space. The work of reading the data can be split between both drives, improving performance. However, with the increased read speed, a RAID 1 implementation loses some write speed.
RAID 5	RAID level 5 spreads data byte by byte across multiple drives, with parity information also spread across multiple drives. You need at least three physical disk drives that have the same capacity and are the same type. If one drive fails, the parity information on the remaining drives can be used to reconstruct the lost data. In the event of a drive failure, data recovery is not instantaneous (as it is in RAID 1); the bad drive needs to be replaced, and then the missing data needs to be reconstructed. With RAID 5, disk performance is enhanced because more than one read and write can occur simultaneously. However, the parity calculations create some write-performance overhead. Storage overhead is at a ratio of one to the number of drives in the set (for example, 1/3 overhead in a three-drive set or 1/10 overhead in a 10-drive set), so the more drives that are in the set, the less overhead, and the better performance. In the event of multiple drive failures, all data will be irrecoverable.
RAID 10	RAID 10, or RAID 1+0, combines two RAID levels into one. It uses RAID 1 and RAID 0 to provide both mirroring from level 1 and striping from level 0. RAID 10 uses a minimum of four disks, in two disk mirrored blocks. This configuration gives you better performance and system redundancy.

Internal Storage Device Considerations

There are several things to consider when you are installing an internal storage device in a computer system. It is not as simple as just plugging the device into the slot inside the case. Make sure you consider each factor before installation.

Consideration	***Details***
Does the computer have existing internal storage devices?	If it does, what interfaces do these devices use (PATA, SCSI, or SATA)? Is there room on the controller of these devices for an additional device? For example, if the computer uses devices with the SATA interface, are there already two devices connected to the controller? If there are, you will need to purchase an additional SATA controller before you can add another SATA device. If you do not have room on the controller for an additional storage device, you must purchase both the storage device and a controller. In addition, make sure that the computer has an available slot for the controller.
Does the device need additional drivers installed?	Make sure that you have the appropriate operating system device drivers to install the new storage device on the computer. If necessary, download the device drivers from the device manufacturer's website.
Does the computer have an available power supply cable to supply power to the device?	If not, you can purchase splitters to enable two (or more) devices to be connected to a single power connection, but be aware of power consumption. The number of connectors approximates the available power, so make sure that the storage device will not cause the computer to exceed the capacity of its power supply.
Does the computer have an available drive bay for the storage device?	Most hard drives require a 3.5-inch drive bay; most tape drives and optical drives require a 5.25-inch drive bay. If you want to install a hard drive in a 5.25-inch drive bay, you will need *drive rails*. Make sure you place the storage device where it will get good air flow to avoid overheating the device. Consider the placement of the drives inside the bays with the cable configurations. You may need to adjust the placement of the drives to match the order of cable connectors.
Do you have the necessary data cables to connect the	SCSI devices require unique SCSI IDs. *SCSI IDs* are assigned to each device connected to the bus. The ID numbers range from 1 to 15, and determine the device priority. Some storage devices require you to configure this ID using a jumper or the device's installation software.

storage device to the controller?	PATA (IDE): Internal PATA hard drives must be jumpered properly. If the drive is the only drive in the computer, you must jumper it as a single drive. If the drive is the second drive in the computer, you must jumper the drive as the second (slave) drive in a two-drive configuration and the first drive as the master drive.
Does the placement of the device interrupt the air flow of the case?	Make sure there is enough total air flow to handle whatever heat the new storage device will add to the computer.

External Storage Device Considerations

External storage devices have a whole set of different considerations than internal devices. Make sure to verify all the factors before selecting and installing a new device.

Consideration	*Details*
What interface does the external storage device require (USB, FireWire, or SCSI)?	• If the external storage device uses USB 2.0, does the computer support it? • If the external storage device uses FireWire, is there an available FireWire port in the computer? If not, you must buy and install a FireWire controller. Make sure the computer has an available slot for the FireWire controller before purchasing one. • If the external storage device uses SCSI, is there room on the SCSI chain for an additional device?
Do you need a cable to connect the external storage device to the computer?	Depending on the type of interface used, you will need to make sure that you have a compatible cable to connect to the computer. Common cable connections include: • USB • FireWire • eSATA • Ethernet
Do you have an available source of power for the storage device?	Some external storage devices will require an additional power source from the computer. For example, eSATA requires an additional power connection to function.

USB Performance Factors

To get the best possible performance from a storage device that uses USB as a connection method, connect it to a port or hub that supports USB 3.0. Keep in mind that many hubs drop all ports down to the slower USB 1.1 speed if you connect any USB 1.1 devices. Try not to connect a slower-speed device to the same hub in which you plan to connect a USB 3.0 storage device.

LearnTO: For additional information, check out LearnTO **Install Storage Devices** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure Storage Devices**

ACTIVITY 4-11: Installing an Internal Storage Device

Before You Begin

To complete this activity, you will need the following hardware components. If you do not have these available, you can remove and reinstall the existing hardware:

- A second hard drive and an empty drive bay. If you have a PATA drive, you will also need an available connection on the PATA cable. If you have a SCSI drive, you will also need an installed SCSI HBA.
- An available power connection for the device you are adding to the system.
- Optionally, rails to allow smaller drives to fit into larger drive bays.

Scenario

You have been assigned the task of refurbishing a computer for a client. This computer has a single functioning hard drive, and the user needs a significant amount of local storage space.

1. Locate the available bay and the power and data connections for the new hard disk drive.
    a. Power off the system, unplug all the peripherals and power cord, and open the computer case.
    b. Locate an available drive bay and determine if the bay is the same form factor as the drive. If you are using a 5.25-inch drive bay and a 3.5-inch drive, you will need to install the drive using rails to adapt the drive to the larger bay.
    c. Locate an available data connection on the data cable. If necessary, connect a PATA data cable to the PATA controller connection on the system board.
    d. Locate an available power connector. If necessary, connect a power splitter to an existing power connection.
2. Prepare the drive for installation.
    a. If you are installing a PATA drive, set the jumpers or switches to Cable Select or slave.
    b. If you are installing a SCSI drive, set the SCSI ID to an unused ID number. If the drive is at the end of the SCSI chain, terminate the device and, if necessary, remove termination from the previously terminated device.
    c. If necessary, attach rails to the drive to fit in the bay.
3. Install the hard disk drive into the system.
    a. Slide the drive into the bay.
    b. Connect the data cable to the drive.
    c. Connect the power cable to the drive.
    d. Secure the drive to the bay chassis with screws.
4. Check whether the drive is accessible.
    a. Plug all the peripherals back into the system.

> **Note:** You can leave the case open until the end of the activity.

b. Restart the computer.
c. If necessary, access CMOS, enable the disk, and then exit CMOS and save your settings.

5. Partition and format the new drive as an NTFS drive.
   a. Log on to Windows as ***Admin##*** with ***!Pass1234*** as the password.
   b. Select **Start,** right-click **Computer,** and select **Manage.**
   c. In the left pane, select **Disk Management.**
   d. If the **Initialize Disk** window is displayed, select **MBR** if the new drive is smaller than 2 TB or **GPT** if the drive is larger than 2 TB. Select **OK.**
   e. If necessary, maximize the **Disk Management** window to view the new drive. It may be labeled **Disk 1 Unallocated.**
   f. Right-click the unallocated space for the new disk.
   g. Select **New Simple Volume.** The **New Simple Volume** wizard starts.
   h. Select **Next.**
   i. In the **Simple volume size in MB** text box, type ***20000***
   j. Select **Next.**
   k. From the **Assign the following drive letter** drop-down list, select **S.**
   l. Select **Next.**
   m. On the **Format Partition** page, verify that **NTFS** is selected and select **Next.**

> **Note:** To save time during class, you can check the **Perform a Quick Format** option.

   n. Select **Finish.**
   o. Close the new drive window.
   p. Close **Computer Management.**
   q. In the **Auto Play** dialog window, click **Open folder** to view files.
   r. Close the **New Volume (s:)** window.

Topic F: Configure the System BIOS

In the previous topics, you focused on the basic internal storage devices that enable a computer to run, but what about how the computer communicates with all these devices? In this topic, you will configure settings in the system BIOS.

How does the computer know when to start devices within the computer? Without the system BIOS managing the system components within the computer system, the devices simply would not be accessible. As an A+ technician, you must fully understand how the system BIOS operates and how to configure it to enable a customized computing environment for users.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.1 Configure and apply BIOS settings.

BIOS Memory

BIOS memory stores information about the computer setup that the system BIOS refers to each time the computer starts. The BIOS information is stored in non-volatile *Electrically Erasable Programmable Read-Only Memory (EEPROM)*, or flash memory chips. Because you can write new information to BIOS memory, you can store information about system changes, such as new components that you add to your system. The computer will look for the component each time it is turned on.

BIOS Components

When the BIOS is activated on startup, it determines which components are present and when they are accessed during the boot process. Any time you change a hardware component, you should check the BIOS settings to see if they also need to be changed for the system BIOS to recognize the new hardware. Also, you can configure BIOS memory without needing to open the chassis. Several system components can be configured through the system BIOS:

- RAM
- Hard drives
- Optical drives
- CPU

Firmware Upgrades

Most modern motherboards contain a number of BIOS chips that contain the system firmware that runs the system BIOS. This firmware may need an upgrade from time to time depending on the manufacturer. When the manufacturer issues an update, then the firmware will need to be updated. These updates contain security patches, updates to the performance, and updates to address any known issues. The updates can be installed in a number of ways, but most commonly can be downloaded from the manufacturer's website and then either burned to CD, or copied to a flash drive.

BIOS Configuration Options

BIOS configuration options can be altered at any time by changing the settings within the BIOS configuration utility. Many times when you replace or change a hardware component, the BIOS configuration will need to be changed so that the system BIOS can recognize the newly installed hardware. System BIOS settings can be configured without having to physically open the system case of the computer. The extent to which you can use BIOS to configure a computer depends heavily on the manufacturer of the particular BIOS; however, in most cases, you should be able to configure at least the following—and possibly much more—from the keyboard by using the BIOS configuration utility.

Configuration Option	***Description***
General	General settings include: • Motherboard information, including the manufacturer, brand, and CPU vendor. • System date and time. You can use the BIOS Setup program to set the PC's real-time clock. (You can also use DOS date and time commands to reset the real-time clock.) • Boot sequence. You can specify the order that drives are checked for the operating system. • BIOS version. This can be used when looking for firmware updates for the BIOS chip.
Security settings	You can specify a number of security functions: • Manage passwords, including both administrator and system passwords. • Enable and disable the trusted platform module (TPM) security feature. When enabled, the BIOS will load the TPM and make it available within the operating system. • In some laptop computers, laptop-tracking software such as LoJack® for Laptops can be configured to help recover lost or stolen laptops.
Memory	Some systems require you to specify in BIOS how much RAM is installed on the system. You might also be able to specify the type of memory used.
	Many devices can be configured by modifying the BIOS settings. You can:: • Specify the type and size of the hard disk drives attached to the system. • Enable and disable advanced drive settings, such as RAID settings.

Enabling and disabling devices	• Specify the preferred default monitor. • Specify settings such as unidirectional or bidirectional printing, Extended Capabilities Port (ECP) options, Enhanced Parallel Port (EPP) options, and what memory addresses and interrupts are used by a port. You can also disable or enable the ports. If you know that a parallel or serial port will not be used, you can disable the port, thereby freeing up the resources that would otherwise be unusable by other devices. Conversely, if you connect a device to a port and the device will not work at all, you might want to check the BIOS to ensure that the port has not been disabled. • Specify settings such as powering down components (like the display device, video card, and hard drives) when the components have not been used for a specified time period, as well as options and time limits for standby and suspend modes. You can also disable or enable global power management.
Clock speed	The clock speed for the CPU can be adjusted in the BIOS. In some modern systems, the CPU type and speed is automatically adjusted, but in older systems, you will verify that the clock speed is optimized for the CPU installed on the motherboard.
System configuration	Allows you to configure various system components such as integrated network interface cards (NICs), USB controllers, parallel ports, and serial ports.
Video	Allows you to change the video controller settings when more than one video card is installed.
Performance	Allows you to change CPU settings such as enabling or disabling multicore support and changing processor modes.
Virtualization support	If the CPU supports virtualization, then you can use the BIOS setup utility to enable or disable the various virtualization settings available. Virtualization support within the BIOS is dependent on the OEM model. Most modern systems will support virtualization.
Power management	Allows you to configure different power options available, such as how the system will recover from a power loss and other advanced power options.
Maintenance	Allows you to verify and set service and asset tags used when a computer needs further maintenance from an outside vendor. The asset tag is used to identify the computer within the BIOS. It is usually a four or five digit number.

LearnTO: For additional information, check out LearnTO **Work with the System BIOS** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

BIOS Diagnostics

Most BIOS systems come with a built-in diagnostics utility that can be used to troubleshoot issues and verify proper functionality. Most diagnostic tools allow you to test the system memory and the entire system. The tool will thoroughly test each system component and display test results which are usually a pass or fail. This will help you to identify which component is having issues. Most utilities will run tests on the following components:

- Video cards
- System memory
- Hard drives
- Optical drives

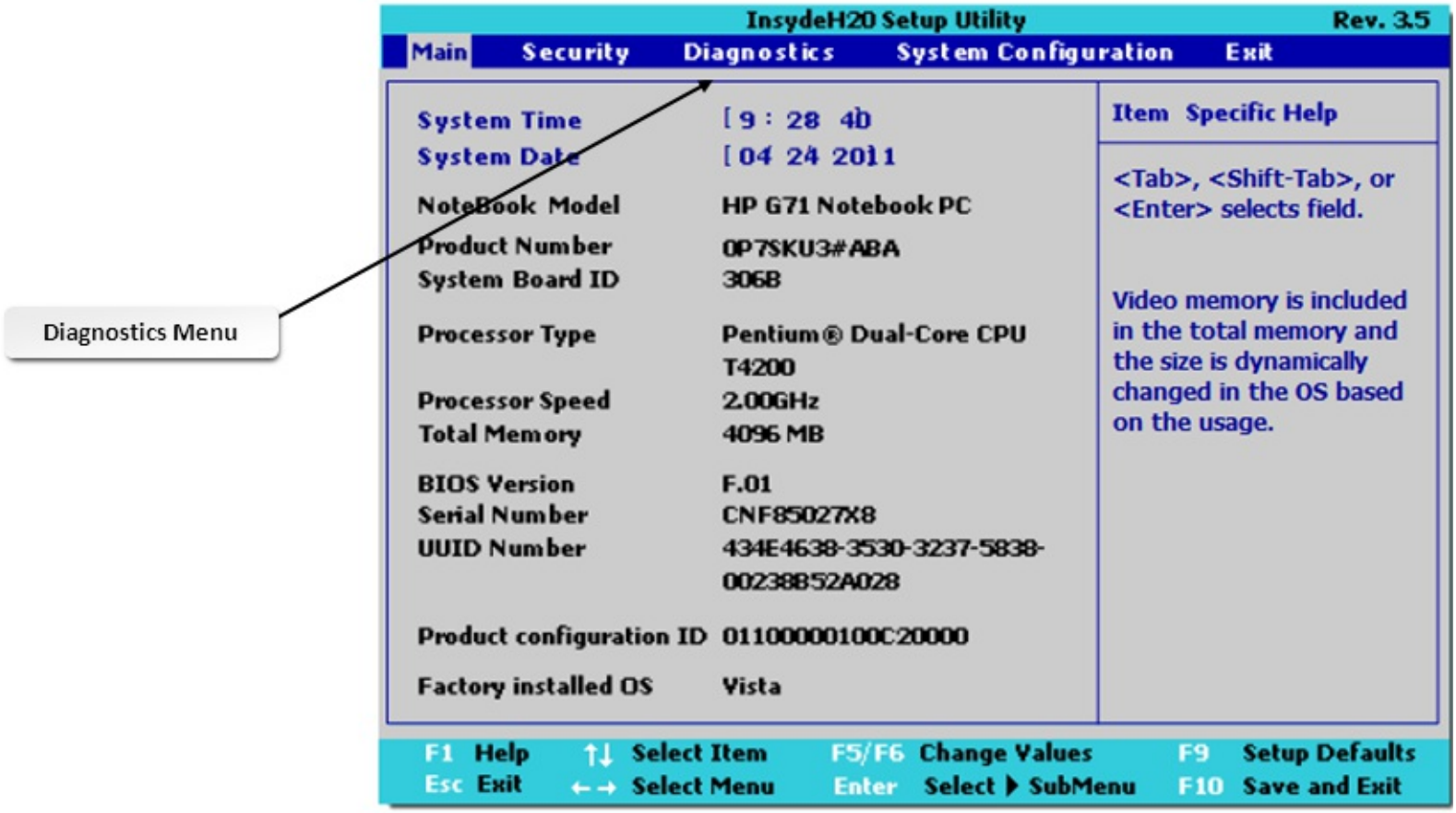


Figure: A sample BIOS diagnostic utility.

BIOS Monitoring Capabilities

Most BIOS have monitoring capabilities built in and can allow you to check a number of system activities for issues. To access the monitoring options, you must enter the system BIOS during start up, by pressing one of the function keys. The specific function key will depend on the type of motherboard installed, so verify the key you need to press on startup to access the BIOS.

Monitoring Capability	***Description***
Temperature	The temperature of the CPU, motherboard, and overall system can usually be checked within the system BIOS. You can use this options to check for overheating and to verify that the CPU is running within its safe temperature range.
Fan speeds	Within the BIOS, you can verify the fan speed for your CPU, and any system fans installed in the computer. Keep in mind that you must balance the rotations per minute (RPM) speed of the fans with the temperature of the CPU and motherboard.
Intrusion detection	Most modern BIOS will have some security functions built in. This includes system intrusion detection. The intrusion detection is implemented using a sensor that alerts the system BIOS when the case cover of the system has been removed.
Voltage	The system voltage settings are strictly based on the specific hardware you have installed in the system, such as type of motherboard and CPU. The BIOS allows you to change the voltage configuration for each device installed. Once in the BIOS, you will look for: • Vcore, or VCC, which is the CPU voltage reading. • Memory voltage, which displays the RAM voltage settings. • VDD voltage, which displays the motherboard's voltage. This rating is driven by the Northbridge chip of the board. • If there is a graphics card installed, then you will see the AGP voltage setting displayed.
Clock	You can verify that the BIOS clock is accurate by verifying the time within the system BIOS.
Bus speed	In some cases, you may find the need to monitor the bus speed, and to make sure that the overall CPU speed is in line with the bus speed. Bus speeds are usually set by the manufacturer at a natural clock rate or an enhanced clock rate. For an example, when you have a processor with a CPU speed of 1.82 GHz clock speed, you would need to set the bus speed to 166 MHz with the multiplier of 11. (166 MHz x 11 = 1.826 GHz).

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Configure System BIOS Settings**

ACTIVITY 4-12: Exploring and Configuring the System BIOS

Scenario

In this activity, you will explore the configuration options available to you in the system BIOS utility.

1. Explore the system BIOS utility.
   a. From the **Start** menu, restart your computer system.
   b. As the computer restarts, press the BIOS access key. You might want to record this key for later use.
   c. Navigate to the **System Setup** menu option. Depending on the BIOS installed on your computer, this menu might have a different name.
   d. Browse through the available BIOS configuration options.
   e. Locate the motherboard settings and record the BIOS version. This information can be helpful if you ever have to update the BIOS to solve a hardware issue.
2. Change the boot order.
   a. Navigate to the **Boot Sequence** setting. Depending on the BIOS installed on your computer, this setting might have a slightly different name.
   b. Examine the current boot order. In older systems, the floppy drive was often configured as the primary boot device. In newer systems, a USB storage device or the internal hard disk might be configured as the primary boot device.
   c. Change the boot order to the following:
      - Optical drive
      - Internal hard disk 1
      - Internal hard disk 2
      - USB storage device
   d. Save the change.
3. Update the system date and time.
   a. Navigate to the **Date and Time** setting. Depending on the BIOS installed on your computer, this setting might have a slightly different name.
   b. Examine the current setting. If the date and time appear to be correct, you can skip this and the next substep. If the date and time are not correct, adjust them to match the current date and time.
   c. Save your changes.
4. Examine system monitoring options.
   a. Navigate to the **Hardware Monitoring** menu option. Depending on the BIOS installed on your computer, this setting might have a different name, such as **PC Health, CPU Temperature,** or some other name.
   b. Examine the CPU temperature reading. Normal CPU temperatures range from 30 to 60 degrees Celsius.
5. Verify the BIOS changes.
   a. Exit the BIOS utility.

b. Log on to Windows.
c. If you changed the date and time, verify that the system date and time has been updated in the taskbar.

Summary

In this lesson, you installed and configured internal system components. In your role as an A+ technician, you will be responsible for helping users with installing motherboards, RAM, CPUs, and storage devices, so having the skills to install and configure them correctly will be crucial to assisting users.

In your current job role, what system components have you worked with the most?

In future job roles as an A+ technician, what system components do you think you will be working with the most?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 5: Customized Client Environments

Lesson Time: 45 minutes

At this point in the course, you have identified the different components that make up a standard workstation. With this information, you are ready to take a look at the hardware needs and requirements for different client configurations. In this lesson, you will identify the different hardware and software needs based on job tasks and functions.

As an A+ technician, you must be knowledgeable in many different areas of information technology. This may include supporting a wide variety of client configurations, such as gaming, audio and video workstations. You must be prepared to fully support any type of environment including more specialized hardware and software configurations based on job roles and tasks.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Topic A:
  - Objective 1.9

- Topic B:
  - Objective 1.9

Topic A: Standard Clients

Now that you have identified the main components of a personal computer, you can start to take a look at what requirements are needed to install and configure a standard client. In this topic, you will identify the hardware and software needs to install a thin client, a thick client, or virtualization workstation.

When installing and configuring user workstations, it is important to identify what the specific needs are of the user that will be using the workstation to perform job tasks. Standard clients are a good starting point for any installation and must be examined to verify that it fits the requirements of the job function.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.9: Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs.

What is a Standard Client?

Standard clients are user-end computers that are administered and managed centrally by a server. Clients will typically include various hardware features and applications that suit the specific needs of the user. Client machines are generally referred to as either thin or thick, depending on the requirements. A *thin client* is a system that relies heavily on another system, typically a server, to run most of its programs, processes and services. On the other hand, a *thick client,* also referred to as a fat client, performs most or all computing functions on its own.

Client Requirements

Client setup requirements will be specific to a user's needs and will most likely be based on a job role. There are however general requirements for each type of client:

Thin Client Requirements	***Thick Client Requirements***
The system must meet the minimum requirements to run a Windows operating system.	The system must meet the standard requirements for running a Windows operating system.
The system uses basic applications that can be accessed over the Internet. The applications do not get installed on the computer and do not use up any hard drive space. RAM is used to run the application from the server.	Full application versions are installed and run directly from the client machine using its own resources. The applications are installed using traditional methods and are stored on the hard drive.
Must have a fast network connection to access the server that is hosting the applications.	If data is stored locally, then access to storage locations is a required with a consistent pathway to data.
Might require specialized software in order to access the applications hosted by the server.	If data is stored on the network, then a consistent path should be established to the storage location with proper security implementations.
May require a specific browser in order to run any web-based applications.	Hardware should be robust enough to run all required applications.

Virtualization Workstation

A virtualization workstation is a system that utilizes both hardware virtualization and client virtualization resources to provide a single virtualized workstation for users. The virtualized workstation is configured to use the system's hardware functions such as access to the graphics card, Random Access Memory (RAM), and Network Interface Card's (NIC's), as well as run the software that provides multiple virtual machines (VMs). Organizations may use virtualization workstations to reduce the use and cost of hardware and to provide employees with a wide variety of OS specific applications from a single workstation. Virtualization provides users with a variety of applications and resources by offering multiple platforms within a single system.

Common virtualization workstation software offerings include:

- VMWare® - **http://www.vmware.com/**
- Oracle®'s VirtualBox - **https://www.virtualbox.org/**
- Microsoft®'s Virtual PC - **http://www.microsoft.com/windows/virtual-pc/**
- Microsoft's Hyper-V® hypervisor (running on the server)

Virtualization Workstation Requirements

Virtualization software vendors will all have specific hardware and system requirements based on their actual software needs, but in most cases will require a virtualization workstation to have:

- The maximum RAM the motherboard can support.
- Maximum central processing unit (CPU) cores.
- Virtualization operating system (OS) if the local personal computer (PC) will be the VM host or virtualization client software installed on the PC if the VM is hosted on a server.
- Fast network connection for server-side VM hosting.

ACTIVITY 5-1: Identifying Standard Client Components

Scenario

You have been asked by your manager to evaluate the hardware and software needs for all the clients within the Human Resources (HR) department of your organization. There was a recent reorganization of the department and some of the job roles and functions have changed. Based on the recent changes, you need to review the job functions and identify what type of client workstation will meet those needs.

1. **The manager of the Human Resources department needs to be able to access the central employee data repository to run reports, but will not need access to the data entry application used to create, edit, and manage the employee data. The employee data is managed on a server that can be accessed with a log in. What type of client is best in this case?**

   _x_ Thin client
   __ Virtualization workstation
   __ Thick client

2. **June has recently been put in charge of making updates to the Human Resource employee benefits website. She will be publishing a monthly newsletter and posting company wide announcements, among other small updates and changes on a regular basis. All changes to the website must be tested on a number of platforms and web browsers to verify that the changes are correct regardless of the operating system and browser. What type of client setup would you suggest for her?**

   A: Answers will vary, but will most likely include a virtualization workstation so that she can switch from different operating system and test any website changes quickly.

3. **In order to properly support the HR employee benefits website, a new server running client VMs has been installed so that the environment that the application requires can be strictly administered by IT staff. Current PCs will be used to access the Client VM environment that is configured on the VM Server. What needs to be present at all PCs that will be accessing this new server and application??**

   _x_ Appropriately configured VM Client.
   _x_ Fast network connection to server hosting the VM environment.
   __ Upgrade to video cards.

4. **True or False? The HR manager's client computer must meet the recommended requirements to run Windows 7 so that she can access and use all of the HR related**

applications used by the organization. In this case, the best client option is a thick client.

_x_ True
__ False

Topic B: Custom Client Environments

The next logical step in examining custom computing environments, is to take a closer look at some of the more specialized environments based on a specific function. In this topic, you will identify the hardware and software needs for various custom computing environments.

There are a wide variety of job functions within the job force, and you may find yourself having to support more specialized computer hardware and software installations. This may include media, audio, and even home entertainment systems. As an A+ technician, you must have the knowledge to provide support in any computing environment.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.9: Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs.

Media Design Workstations

Media design workstations are configured to support the needs of graphic designers, Engineers, architects, 3D media developers, and other design driven job roles. The workstation's hardware and software needs will be dependent on the specific programs and computing tasks required by the job role.

Figure: A media design workstation.

Media Design Workstation Requirements

Media design workstations require a specific set of requirements. Actual hardware and software requirements will depend on the user's specific job role and function, but most media design workstations will require a similar set of tools and components.

Common hardware components include:

- A powerful processor.
- A high-end video/graphics card with integrated *Graphics Processing Unit (GPU)*.
- Large flat panel display, or multiple monitors.
- Maximum RAM supported by the motherboard and CPU.

Common software applications include:

- Adobe's Creative Suite.
- 3D Studio Max.
- Computer aided design (CAD) programs.
- SharePoint.

GPUs

The GPU (graphics processing unit) is an electronic circuitry unit that alters and controls the memory of a computer to meet the immediate needs of rapidly changing computer graphics and detailed visual images displayed on the display device. There are a number of ways GPUs are implemented within a computing device depending on the specific needs of the user and applications. Most modern PCs, laptops, and some mobile devices come with a GPU already installed on either the motherboard or the CPU. The most powerful GPUs are considered to be high-end specialized units that come already installed on the video card and have various output methods and capturing devices.

CAD Design Workstations

CAD workstations are unique in that they require both the hardware and the software on a system to meet certain requirements to produce complex 3D designs. CAD workstations require a high-end graphics card and monitor, and specialized input devices such as, a digitizing tablet and light pen. Industries that use CAD created design specifications include the automotive companies, aerospace, and architectural firms.

CAM Design Workstations

Computer aided manufacturing workstations are a type of workstation that is set up with specific hardware and software that can control machine tools found in manufacturing environments. Specialized controller cards may be required as well as specialized connections and software. CAM machines may be installed in harsh environments—such as manufacturing buildings and automotive factories—so the environments may need to be hardened machines that will not be aversely affected

by harsh working environments.

Audio/Video Editing Workstations

An *audio/video editing workstation* is a powerful computer setup that supports editing of audio and video recordings. These systems must be able to support the demanding editing programs that audio/video technicians use in post production editing functions. Most professional videos taken today include special effects and CGI (computer generated imagery) that is all applied after the digital video is taken. Common applications found on an audio/video editing workstation include:

- Sony's Vegas Pro.
- Apple's iMovie.
- WavePad.
- Corel's VideoStudio Pro X5.
- Adobe's Premiere Elements.
- AVS Audio Editor.
- MAGIX Movie Edit Pro and Music Maker.
- CyberLink's PowerDirector.

Figure: An audio/video editing workstation.

Audio Video Editing Hardware Requirements

The hardware and software requirements for each individual audio/video editing workstation will differ depending on what specific tasks the job role will need to do. Most stations will require the following hardware components:

- A specialized audio and video card to support CGI and 3D post production effects.
- A large fast hard drive.
- A high-end general processing unit (GPU).
- Large flat panel or multiple displays.

Gaming PCs

A *gaming PC* is a computer that comes equipped with powerful graphics capabilities, fast processing capabilities and a large amount of memory. The main difference between a gaming PC and other consumer workstations is that they are specifically designed and built to support the demanding computing requirements by gaming software applications. All gaming PCs will require a high-end GPU to support the detailed 3D graphics and realistic imagery presented in PC games today. Gaming platforms are also popular today and provide gamers with a number of application options, message boards, and files sharing via an online portal, such as Steam™ and Origins™.

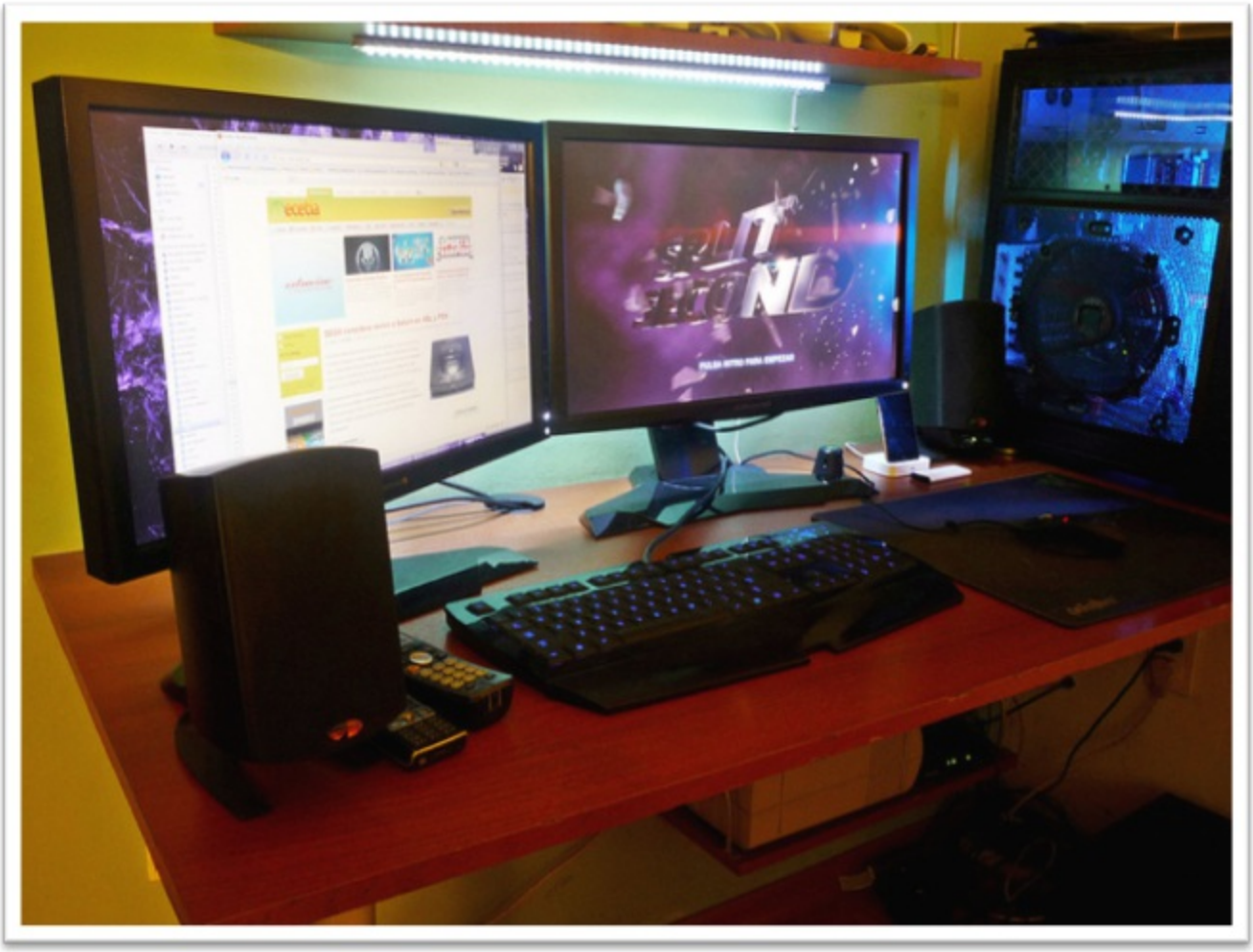


Figure: A gaming PC.

Popular gaming software applications include:

- Diablo® III
- StarCraft® II: Heart of the Swarm
- Dota™ 2
- Guild Wars® II

Gaming PC Requirements

There is such a wide variety of gaming software applications, so each gaming PC will have specific requirements based on the needs of the user and the applications used. Gaming PC's require very specific components in order to support the demands of gaming software. Common requirements include:

- A powerful processor.
- A high-end video/specialized GPU unit.
- A high quality sound card.
- High-end cooling such as a water cooling system.
- Maximum RAM that is supported by the motherboard.
- Fast Internet connection for interactive gaming needs.
- Real-time video and audio input/output capabilities.
- In some cases, HDMI output.

Gaming Peripherals

There are many different peripherals used within the gaming world. The most common ones include the mouse and keyboard, but there are others that may be used depending on the type of game played:

- Gaming mice that are wireless and include many buttons and different ergonomic form factors.
- Customized keypads, with moveable keys.
- Steering wheels used for auto racing games.
- 3D glasses.
- Specialized gaming mouse pads.
- Specialized audio system.
- PC video camera.

Home Theater PC

A *home theater PC (HTPC)* is a computer system that is dedicated and configured to store and stream digital movies, either from the local hard drive or through an online subscription such as Netflix. Other capabilities include connecting and managing surround sound audio and speakers and DVR, or digital recording functions. The HTPC is usually equipped with specific entertainment software that can be used to manage the music and video files stored on the computer. The PCs are generally located near the TV and other home entertainment devices and have a HTPC form factor, which is aesthetically appealing and designed to look similar to other home entertainment devices. They are also designed to be less noisy that a traditional PC, with more compact quieter cooling methods and the addition of sound dampening foam or padding to limit excessive noise generated by the fan and hard drive.

Figure: A home theater PC.

Home Theater PC Requirements

Home Theater Personal Computers (HTPCs) are built specifically for home theater purposes, so most of the required elements are built right into the actual system. They generally include:

- A TV tuner card that allows the computer to display high-definition (HD) digital output and attach the cable provider's cable TV wire directly to the system.
- A cable card, that provides authentication and encryption services to connect with the cable set top box provided by the cable company.
- Optical disk player that supports both DVD and Blu-ray.
- Maximum RAM supported by the motherboard.
- Video card with both GPU and HD capabilities.
- Bluetooth® or wireless capabilities when using specialized remotes or input devices.

Movie Players

There are a number of software applications available for playing HD movies on a HTPC including:

- Cyberlink PowerDVD.
- XBMC Media Center.
- Windows Media Center.
- Boxee.

Home Server PC

A home server PC is a server for your house that is connected to multiple computing devices within the home to store videos, music, and pictures. It also provides central access to all stored files and is often used for file and print sharing with other computing devices in the home. The home setup generally includes a wireless network that all devices can connect to provided by a home wireless router. This allows any device to access the server within the home.

Figure: A home server.

Home Server Requirements

Each home server PC will have a variety of features and functions, but when it comes to requirements they all have common requirements for providing a home with necessary functions:

- Media streaming capabilities to access and play digital movies.
- File sharing for all home users to access the file system on the server.
- Print sharing.
- A gigabit NIC to provide the speeds necessary to perform large file transfers over the wireless network.
- Router that is compatible with the gigabit speed required by the NIC in the server.
- Redundant Array of Independent Disks (RAID) array to provide redundancy.

ACTIVITY 5-2: Selecting a Custom Client Configuration

Scenario

You are a support technician for a local business that specializes in consulting, purchasing, and installing home computing solutions for consumers. You are responsible for fulfilling all the orders that have come in overnight through the business' website.

1. **Customer 1 is using a desktop PC to play home movies and to set up slide shows to show his family their vacation photos and is having difficulty with the computer freezing during the movies. He is looking for a solution that will allow him to store and play his movies seamlessly through a computer. He also wants his wife to be able to access the pictures and movies from her laptop within the house. What type of computer setup would you suggest for this customer? What specific questions might you ask this customer about additional component needs?**

   A: Answers may vary, but will most likely include setting up a home server PC for easy file sharing among the household computing devices and to provide more speed to play movies from the PC. You may ask if they are in need of additional storage space and if they are looking for redundancy through a RAID array in the PC.

2. **Customer 2 is from a small real estate office who has recently hired a Graphic Designer to produce informational pamphlets and other marketing materials for the agency such as, property drop sheets and circular layout designs. The office manager has asked your company to determine the hardware and software needs for the designer's workstation so that it can be ordered and set up before their scheduled start date in two weeks. What hardware and software requirement you would suggest for the Graphic Designer's workstation?**

   A: Answers may vary, but will most likely include a PC with a newer powerful processor such as an Intel Core i7, a high end video card, and the maximum RAM that the motherboard can handle. The applications will most likely include Adobe's Create Suite of products.

3. **Customer 3 is looking to make the switch from a traditional cable box, DVD player to a home theater PC, so that she can stream Netflix and DVR shows and movies from her TV. She already purchased a HTPC from a local home entertainment store but cannot figure out how why she cannot connect the cable TV wire into the HTPC. What required component might be missing that would enable her to make the connection?**

   A: The TV tuner card installed in the HTPC. The tuner card provides the port to connect the cable from the provider to the HTPC.

Summary

In this lesson, you identified all the different components needed to provide a custom computer setup that is based on specific user needs. There is a wide variety of job functions within the corporate world today, so identifying specific hardware and software needs based on a users job role will only help you in providing the right level of support within your organization.

Have you had any experience with any of the workstation or server setups presented in this lesson?

What types of custom client setups do you think you will encounter the most in your role as an A+ technician?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 6: Networking Technologies

Lesson Time: 4 hours, 5 minutes

In this course, you are learning to support a wide range of computing device features and functions. A key factor in device communication is how they are connected and how they transfer data to one another. In this lesson, you will identify a number of networking technologies.

Just about very digital device on the planet today is connected to external resources via some kind of network, whether it is a small office/home office (SOHO) network, a corporate wide area network (WAN), or directly to the Internet itself. The ability to connect, share, and communicate using a network is crucial for running a business and staying connected to everything in the world, so as an A+ support technician, you will need to understand the technologies that underlie both local and global network communications to ensure that the organization you support stays connected.

SOHO networks are much like the larger corporate networks, just on a much smaller scale. No matter what the size or location of the network, you are still responsible for understanding how it is structured and configured. A+ technicians must understand the needs and complexities of SOHO wired and wireless networks.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Topic A:
  - Objectives 1.7, 1.11, 2.1, 2.2
- Topic B:
  - Objectives 2.3, 2.4
- Topic C:
  - Objectives 2.7, 2.8, 2.9
- Topic D:
  - Objective 2.4
- Topic E:
  - Objective 1.6
- Topic F:
  - Objective 2.10
- Topic G:
  - Objective 2.5
  - Objective 2.6

Topic A: Physical Network Connections

In this lesson, you will identify various networking technologies. In order to do so, you will need to understand a few basic concepts and the connections used to implement computer networks and their components. In this topic, you will identify the physical network connections that make up most computer networks.

No matter what types of networks you support in your professional career, they will all share some fundamental characteristics as well as basic physical components. As a computer support technician, dealing with these components will need to be as natural to you as handling a scalpel is to a surgeon. The information in this topic will familiarize you with the physical network connections and components that you will deal with on a daily basis as a support technician.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.7: Compare and contrast various connection interfaces and explain their purpose.
- Objective 1.11: Identify connector types and associated cables.
- Objective 2.1: Identify types of network cables and connectors.
- Objective 2.2: Categorize characteristics of connectors and cabling.
- Objective 2.4: Explain common TCP and UPD ports, protocols, and their purpose.

Networks

A *network* is a group of connected computers that communicate and share resources such as files, printers, Internet connections, and databases. Whether wired or wireless, most networks will include network media, such as a cable to carry network data; network adapter hardware to translate the data between the computer and the network media; an operating system to enable the computer to recognize the network; and a network protocol to control the network communication. All these components work together to enable a fully functioning computer network. Any computing device that will communicate with a network will also include a *network interface card (NIC)* that is usually built into most devices. Older devices may require an adapter card that can be inserted into an expansion port or slot.

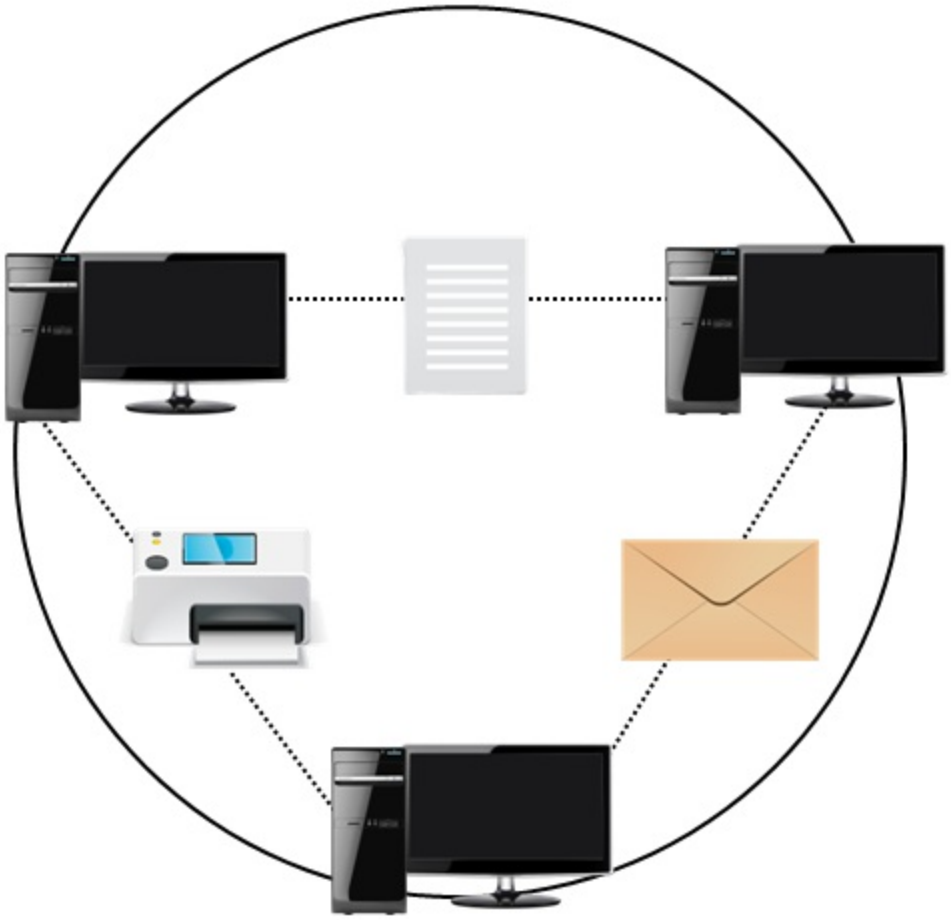


Figure: A network.

Network Models

There are two primary network models, which are design specifications for how the computers and other *nodes* on a network can interact.

Network Model	*Description*
Client-server	A *client/server network* is a network in which computer functionality is divided into two roles: *server* computers, which provide services and control network operations, and *client* computers, which use the services provided by the servers. Typically, there is at least one server providing central authentication services. Servers also provide access to shared files, printers, hardware, and applications. In client/server networks, processing power, management services, and administrative functions can be concentrated where needed, while clients can still perform many basic end-user tasks on their own. Microsoft® Windows Servers® support a client/server network type known as a domain.
Peer-to-peer	A *peer-to-peer network* is a network in which resource sharing, processing, and communications control are completely decentralized. All clients on the network are equal in terms of providing and using resources, and users are authenticated by each individual workstation. Peer-to-peer networks are easy and inexpensive to implement. However, they are practical only in very small organizations, due to the lack of central data storage and administration. In a peer-to-peer network, user accounts must be duplicated on every workstation from which a user accesses resources. Such distribution of user information makes maintaining peer-to-peer networks difficult, especially as the network grows. Consequently, peer-to-peer networks should not exceed 10 computers. A Windows® workgroup is an example of a peer-to-peer network.

Network Interface Card Characteristics

Network interface cards have some special characteristics that distinguish them from other types of adapter cards.

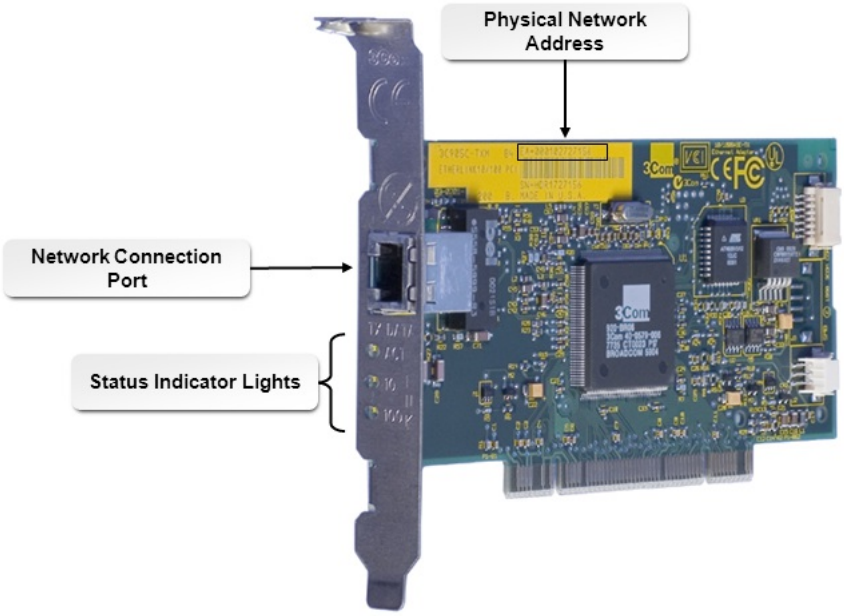


Figure: A network interface card.

Network interface card characteristics are described in the following table.

Characteristic	***Description***
Network connection port	Network adapter cards will have one or more ports that are configured to connect specifically to a given type of network cable. Some older cards had several types of ports so that they could connect to several different types of network cable. Network connections today are standardized and almost all use one port type.
Physical network address	Each network adapter has a globally unique *physical address* burned onto the card by the card manufacturer. The physical address uniquely identifies every individual card that connects to the network cable or media. For this reason, the physical address is also called the *Media Access Control (MAC) address*. MAC addresses are six bytes long. A typical MAC address might appear as **00-00-86-47-F6-65,** where the first three bytes are the vendor's unique ID and the next three uniquely identify that card for its vendor.
	Network adapters, including those built into most network devices, typically have one or more light emitting diode (LED) status lights that can provide information on the state of the network connection. • Most adapters have a *link light* that indicates if there is a signal from the network. If the link light is not lit, there is generally a problem with the cable or the physical connection.

Status indicator lights	• Most adapters also have an *activity light* that flickers when packets are received or sent. If the light flickers constantly, the network might be overused or there might be a device generating network noise. • Some multi-speed adapters have a *speed light* to show whether the adapter is operating at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet). • Some types of equipment combine the functions of more than one light into dual-color LEDs. For example, a green flickering light might indicate normal activity, while an orange flickering light indicates network traffic collisions.

Twisted Pair Cables

Twisted pair is a type of cable in which four pairs of insulated conductors are twisted around each other in pairs and clad in a protective and insulating outer jacket. There may be multiple pairs depending on the type and size of cabling. Shielding can be added around the bundle of twisted pairs to reduce electronic interference.

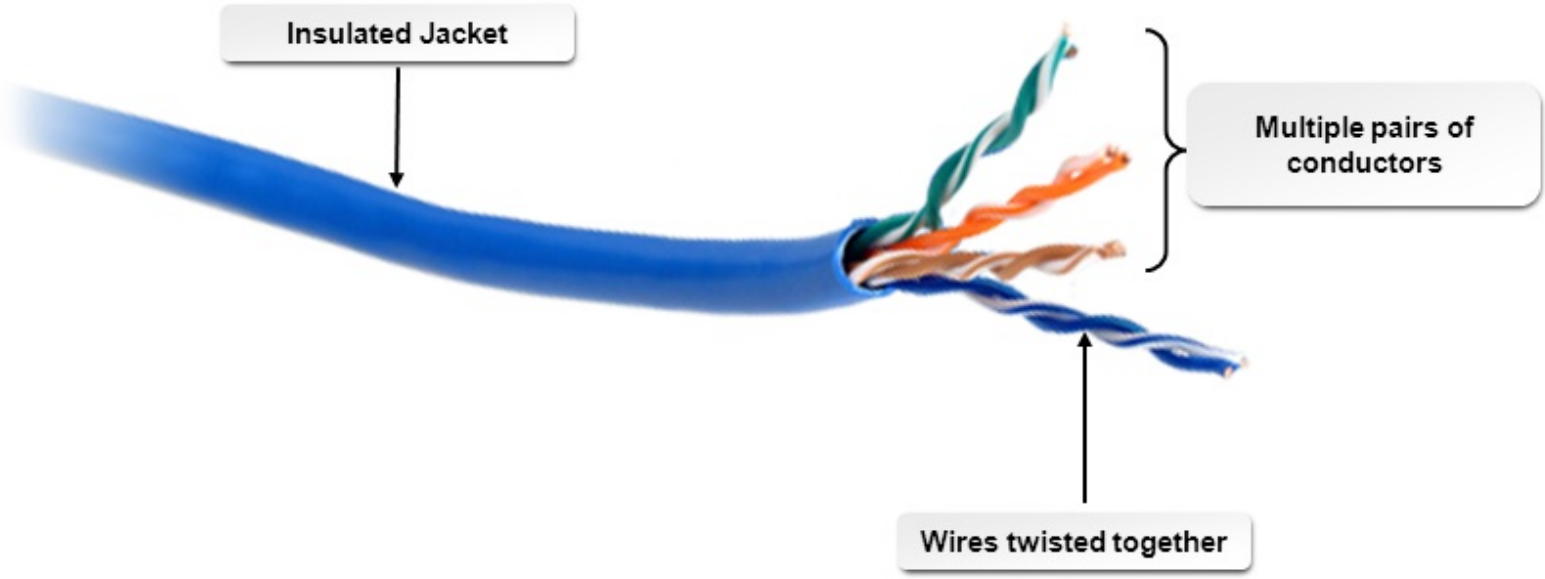


Figure: Twisted pair cable.

Types of Twisted Pair Cable

Twisted pair cable comes in two basic types: unshielded twisted pair (UTP) and shielded twisted pair (STP). As the name implies, STP includes shielding, typically a foil wrapper, around its conductors to improve the cable's resistance to interference and noise. It tends to be more expensive than UTP and is installed only when needed.

UTP cable comes in different grades, called categories, which support different network speeds and technologies. A cable's category is typically printed on the cable itself, making identification easy.

Category	***Network Type and Maximum Speed***
CAT 3	• Network Type: Telephone or Ethernet • Maximum speed: 10 Mbps CAT 3 is currently used for telephone wiring
CAT 5	• Network Type: Fast Ethernet Maximum speed: CAT 5 supports a signaling rate up to 100 Mbps
CAT 5e	• Network Type: Gigabit Ethernet Maximum speed: CAT 5e supports a signaling rate of 350 Mbps
CAT 6	• Network Type: Gigabit Ethernet • Maximum speed: 1 Gbps CAT 6 supports a signaling rate of 250 MHz
CAT 6a	• Network Type: Gigabit Ethernet • Maximum speed: 1 Gbps CAT 6a supports a signaling rate of 500 MHz
CAT 7	• Network Type: Gigabit Ethernet. • Maximum speed: 1 Gbps+

	CAT 7 supports a signaling rate of 1 GHz

PVC Cable vs. Plenum Cabling

Polyvinyl chloride (PVC) is an inexpensive and flexible rubber-like plastic used to surround some twisted pair cabling. However, when PVC burns, it gives off noxious or poisonous gases.

Plenum cable jacketing does not give off noxious or poisonous gases when it burns. Fire codes require that you install this special grade cabling in the *plenum,* which is a building's air handling space between the structural ceiling and any suspended ceiling, under raised floors, and in firebreak walls.

Twisted Pair Connectors

The RJ45 connector is used on twisted pair cable. RJ45 is an eight-position connector that uses all four pairs of wires. Be careful not to confuse the RJ45 connector with the similar, but smaller, RJ11 connector. The RJ11 connector is a six-position connector that uses just one pair of wires. It is used in telephone system connections and is not suitable for network connectivity. The RJ in RJ11 or RJ45 is an abbreviation for "registered jack."

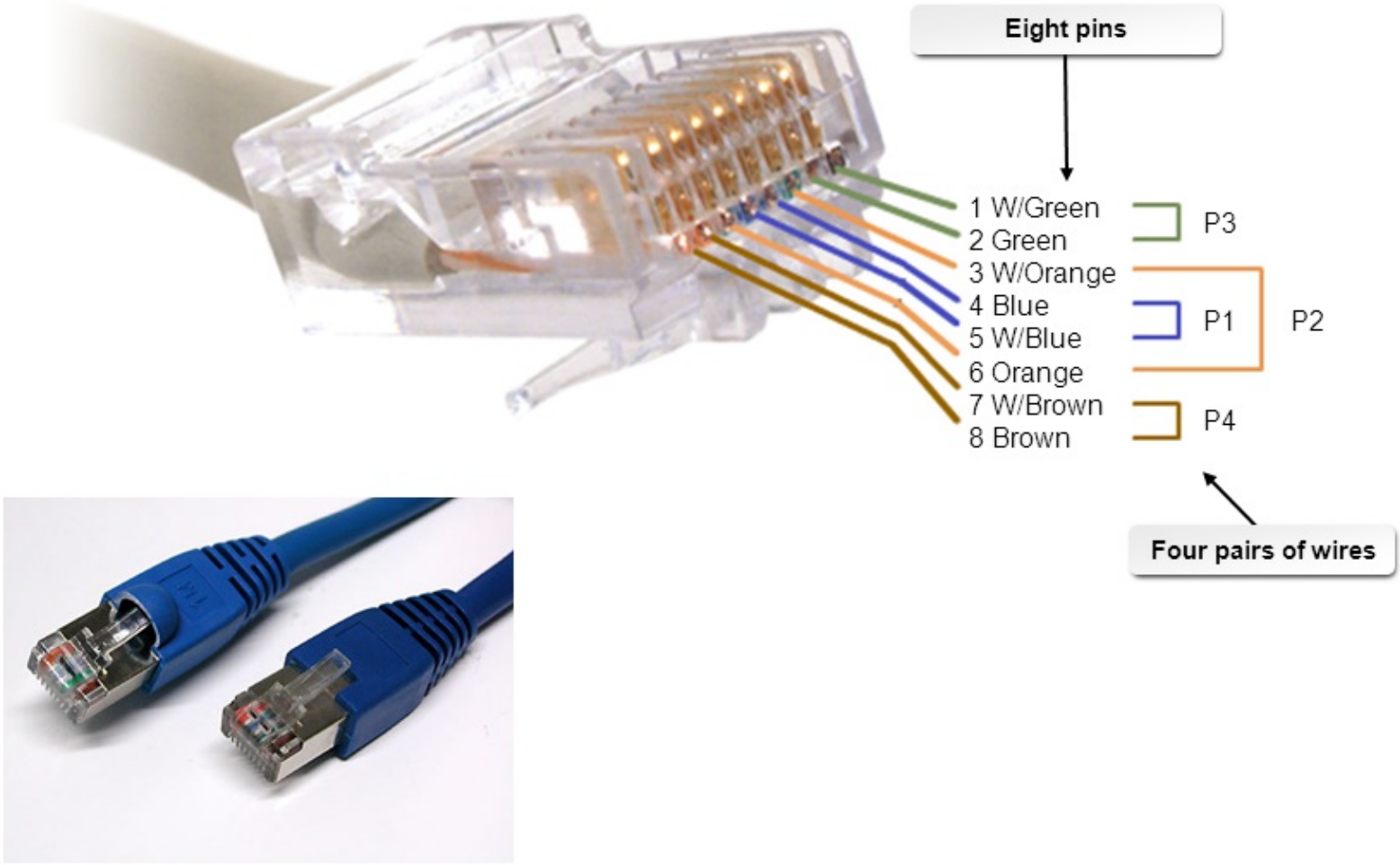


Figure: Twisted pair connectors.

Twisted Pair Wiring Standards

The *Telecommunications Industry Association (TIA)* and the *Electronic Industries Alliance (EIA)* developed the 568 Commercial Building Telecommunication Cabling standard. This standard defines the regulations on designing, building, and managing a cabling system that utilizes structured cabling according to specified performance characteristics to create a system of unified communications.

TIA/EIA releases recommendations for how network media may best be installed to optimize network performance:

- T568A is a legacy standard that was used in commercial buildings and cabling systems that support data networks, voice, and video. It further defines cable performance and technical requirements.
- T568B defines the standards for preferred cable types that provide the minimum acceptable performance levels including:
    - 100 ohm twisted pair cable.
    - Shielded twisted pair cable.
    - Optical fiber cable.
- T568C is the latest standard released by TIA/EIA that is designed to be used in commercial buildings and in multiple locations and to provide full support for all modern and future communications needs.

Coaxial Cables

Coaxial cable, or *coax,* is a type of copper cable that features a central conductor surrounded by braided or foil shielding. An insulator separates the conductor and shield, and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

Note: Coaxial cable is so named because the conductor and shield share the central COmmon AXis or are co-axial. This arrangement helps prevent electromagnetic interference from reaching the conductor.

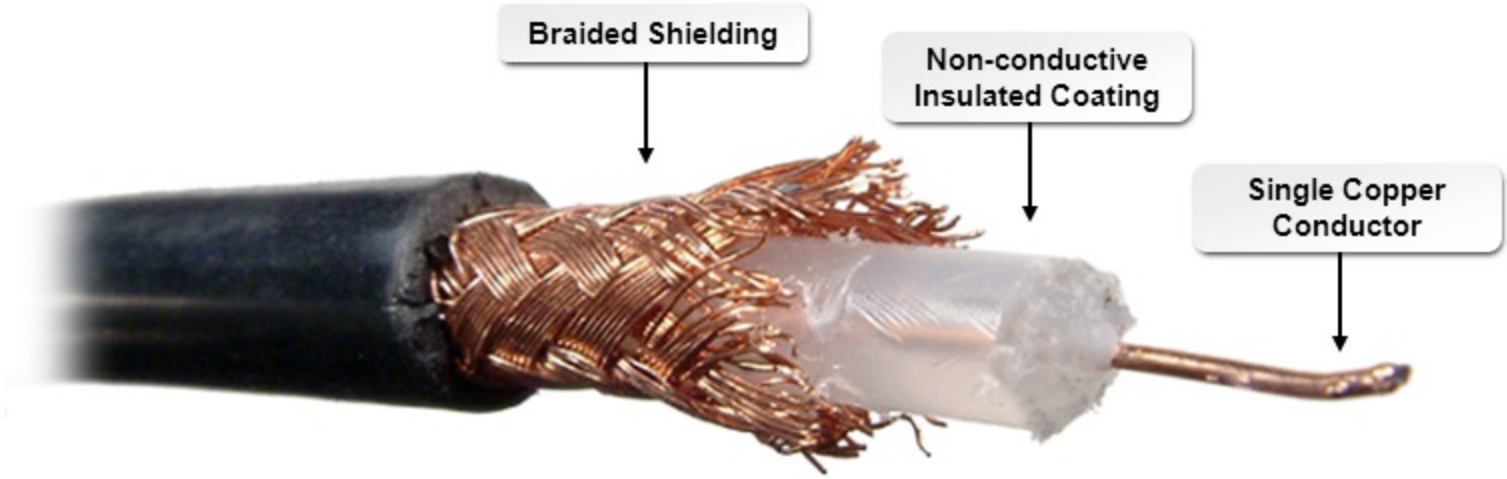


Figure: Coaxial cable.

Coaxial Cable and Connector Types

Coaxial cable comes in various thicknesses that use different connector types.

Figure: Typical Thinnet connectors.

The different types of coaxial cable are described in the following table.

Coaxial Cable Type	***Description***
5 mm/0.25 inch ("Thinnet")	RG-58/U and RG-58A/U, also known as thinnet, are older types of media used for networking. RG-59 is used for cable television transmission. The specifications include a maximum transmission speed is 10 Mbps using baseband transmission up to 185 meters in length. Thinnet connections are made with a twist-lock connector called a Bayonet Neill-Concelman (BNC) connector. Devices connect to the network with T-connectors. Each end of the cable must be terminated with a 50-ohm resistor.

	Another coax connector type is the *F-connector,* which is used to connect cable TV and FM antenna cables. Today, F-connectors are also used to connect cable modems to the CATV network.
6.91 mm/ 0.35 inch	RG-6/U has been replacing RG-59 in recent years as the preferred cable for CATV networks. Like RG-59, F-connectors are used to connect cable modems to the CATV network.
10 mm/0.5 inch ("Thicknet")	RG8 is a thicker type of coaxial cable often referred to as thicknet. It is seldom seen today due to its expense and stiffness, but was popular at one time as a backbone cable in coaxial network installations. The specifications include a maximum transmission speed is 10 Mbps using baseband transmission up to 500 meters in length. Connections between Thicknet segments are made with a screw-type connector called an N-connector. Thicknet segments must be terminated with a 50-ohm resistor. A legacy method used to quickly connect a computer to a thicknet wire is called a vampire tap.

Termination

Coax network segments typically must be *terminated* to prevent signal reflections off the end of the cable. Cables are terminated by installing a resistor of an appropriate rating, typically 50 ohms, on the end of the cable.

Fiber Optic Cables

Fiber optic cable is a type of network cable in which the core is one or more glass or plastic strands. The core is between 5 and 100 microns thick and is surrounded by cladding, which reflects light back to the core in patterns determined by the transmission mode. A buffer, often made of plastic, surrounds the cladding and core. To add strength (or pull strength) to the cable, strands of Kevlar® surround the buffer. An outer jacket, sometimes called armor, wraps and protects the whole assembly. Light pulses from a laser or high-intensity light-emitting diodes (LEDs) are passed through the core to carry the signal. The cladding reflects the light back into the core, increasing the distance the signal can travel without being regenerated.

Fiber optic cables are expensive, fragile, and difficult to install. However, fiber optic transmissions are fast and reliable over extremely long distances, so they are used frequently in backbone wiring solutions. Also, fiber optic cables are impervious to electromagnetic interference.

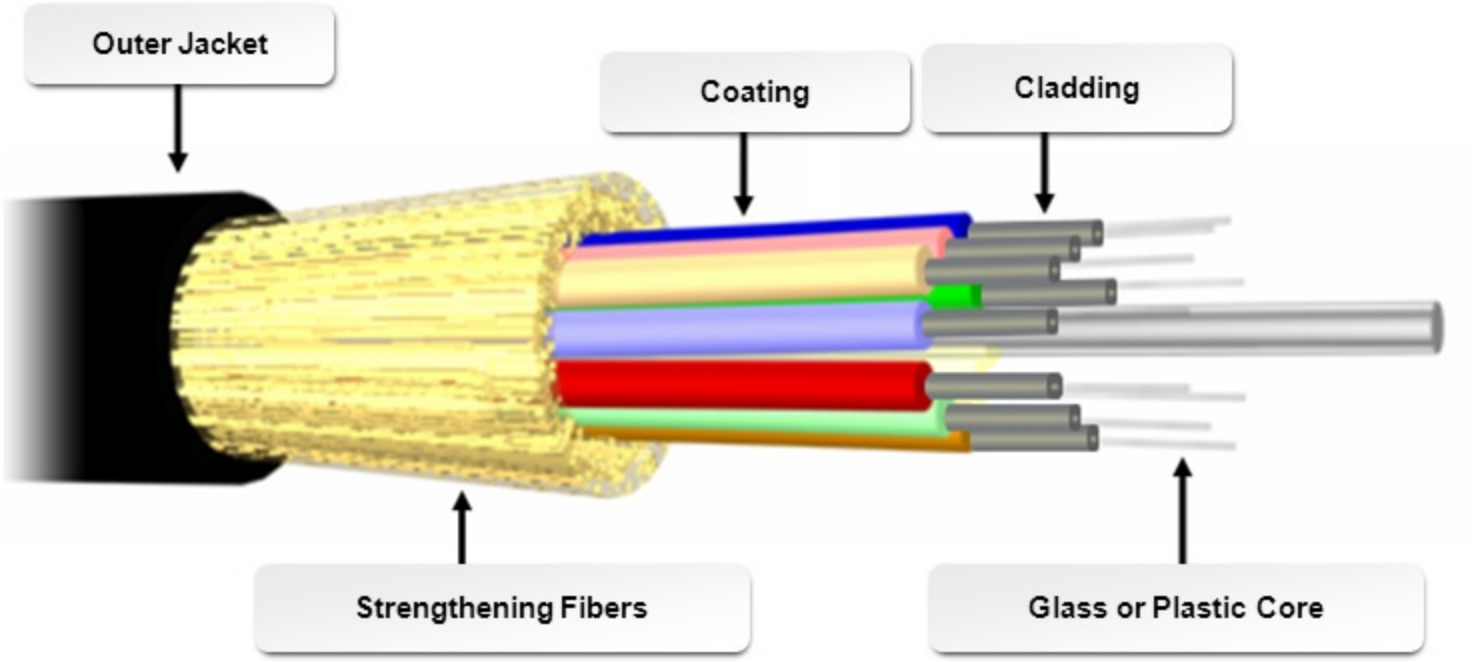


Figure: A fiber optic cable.

Fiber Optic Cable Types

There are two types of fiber optic cables: single-mode or multimode fiber.

Mode Type	*Description*
Single-mode fiber	Carries a single optical signal, and has a small core that allows only a single beam of light to pass. A laser, usually operating in the infrared portion of the spectrum, is modulated in amplitude (intensity) to transmit the signal through the fiber.
Step index multimode fiber	Contains a core surrounded by cladding, each with its own uniform index of refraction. When light from the core enters the cladding, a step down occurs due to the difference in the refractive indices. Step-index fiber uses total internal reflection to trap light.
Graded index multimode fiber	Possesses variations in the core glass to compensate for mode path length differences. It provides up to 2 GHz of bandwidth, which is significantly more than step-index fiber.

Fiber Optic Connector Types

There are various connector types used with fiber optic cable.

Connector	Description
Straight Tip (ST)	Used to connect multimode fiber, ST connectors look like BNC connectors. They have a straight, ceramic center pin and bayonet lug lockdown. They are often used in network patch panels. ST connectors are perhaps the most popular type of fiber connector.
Subscriber Connector or Standard Connector (SC)	Box-shaped connectors that snap into a receptacle. SC connectors are often used in a duplex configuration where two fibers are terminated into two SC connectors that are molded together. SC is used with single-mode fiber.
Face Contact (FC)	Similar to SMA connectors, FC connectors use a heavy duty ferrule in the center for more mechanical stability than SMA or ST connectors. These connectors are more popular in industrial settings where greater strength is required.
Fiber Distributed Data Interface (FDDI)	The FDDI connector is a push/pull type, two-channel snap-fit connector used for multimode fiber optic cable. Also called a MIC (Media Interface Connector).
	A bayonet-style connector using the traditional BNC connection method.

Mini-BNC	
Biconic	The biconic connector is a screw-on type connector with a tapered sleeve that is fixed against guided rings and screws onto the threaded sleeve to secure the connection. When the connector is inserted into the receptacle, the tapered end of the connector locates the fiber optic cable into the proper position. The biconic connector is one of the earliest connector types and is, for the most part, no longer in use.
Local Connector (LC)	The LC is a small form factor ceramic ferrule connector for both single-mode and multimode fiber. It is about half the size of the SC or ST. The LC uses an RJ45-type latching and can be used to transition installations from twisted pair copper cabling to fiber.
Sub Multi Assembly or Sub Miniature type A (SMA)	Similar to ST connectors, SMA connectors use a threaded ferrule on the outside to lock the connector in place. These are typically used where water or other environmental factors necessitate a waterproof connection, which is not possible with a bayonet-style connector.
Mechanical Transfer Registered Jack (MT-RJ)	The MT-RJ connector, sometimes called a Fiber Jack connector, is a compact snap-to-lock connector used with multimode fiber. The MT-RJ is easy to use and similar in size to the RJ45 connector. Two strands of fiber are attached with one connector.

Wireless Connections

Wireless connections are network connections that transmit signals without using physical network media. Instead, signals are transmitted as electromagnetic energy, such as radio waves, satellite microwave, or infrared light. Most general office wireless implementations use radio. Wireless communication enables users to move around while remaining connected to the network.

Note: Wireless communication permits connections between areas where it would be difficult or impossible to install wires, such as in hazardous areas, across long distances, or inside historic buildings. It is also extremely popular in standard business and home installations because of the mobility and flexibility it provides, as well as the simplicity of media-free installation.

Figure: Wireless connections.

Wireless Signal Strength

The ability to communicate via wireless network is highly dependent upon the local signal strength. Signal strength can vary in relation to a number of factors, including interference and distance from the Wireless Access Point (WAP). Most wireless devices will provide some kind of indicator regarding the strength of the current wireless signal. For example, in Windows, a wireless network card will display a message on screen when signal strength is low and connectivity is limited as a result.

Wi-Fi

Wireless radio communications following the IEEE 802.11g Wi-Fi standard are the most common choice for ordinary wireless LAN connectivity for portable computers inside homes, offices, and, increasingly, public buildings. Choose Wi-Fi when you need to connect portable computer systems to a wired or wireless Ethernet LAN and enable users to move from place to place freely without a line of sight to the WAP. Wi-Fi provides good performance within the WAP coverage area, barring any signal interference.

Additional Network Connection Methods

In addition to coax, twisted pair, and fiber optic, you can use other types of cables and methods to make network connections, including USB, FireWire®, and RS-232 null-modem cable. You can also make wireless connections using radio, infrared, or satellite transmissions. Physical network cable connections are often referred to as a group as bounded media. Wireless connection types that transmit signals through the air without a cable are collectively called unbounded media.

RS-232 Null-Modem Connections

RS-232 is a standard serial interface that was used to connect serial devices, particularly modems. These connections have been primarily replaced by the faster Ethernet, but can be found in some cases to connect devices for debugging and to connect devices in close proximity of one another. When you use an RS-232 null-modem cable to create network connections between computers, it mimics the presence of a modem connection between the two systems. There are some types of network connections, such as a dial-up Internet connection, that use telephone media. So, with an RS-232 null-modem cable connected to two computers' serial ports, you can, in effect, create a simulated dial-up connection directly between the two systems.

ACTIVITY 6-1: Identifying Network Cables and Connectors

Scenario

In this activity, you will identify the various types of cables and connectors used to make network connections.

1. Look at the cables and connectors on the back of your computer, and identify what cables are used and what their purpose is.

2. **What type of cable is used to connect your computer to the network?**

   A: Answers will vary depending on the location of the participant and the type of network interface is in the computer, and could range from twisted pair to wireless to virtual.

3. **Are there any LED lights on the cable ports indicating activity?**

   A: Answers will vary depending on the location of the participant and the level of network activity. Some participants might see the LED lights lit or blinking, while others might not.

Topic B: TCP/IP

Now that you are familiar with the basic components that make up a network, you can start to take a closer look into how Transmission Control Protocol/Internet Protocol (TCP/IP) addressing and data delivery methods are used to implement TCP/IP on a network. In this lesson, you will identify the properties and characteristics of TCP/IP.

As an A+ technician, you must be able to identify the components of a system in order to provide the right level of support to your organization. Because all networks are different, you still need to be able to identify the components and how they are connected. Understanding how everything is connected and functioning within the network will allow you to properly support TCP/IP within the network.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 2.3: Explain properties and characteristics of TCP/IP.

What is TCP/IP?

Transmission Control Protocol/Internet Protocol (TCP/IP) is a nonproprietary, routable network protocol that enables computers to communicate over all types of networks. TCP/IP is the native protocol of the Internet and is required for Internet connectivity. TCP/IP is a suite of related protocols that work together to provide network addressing and naming, and data delivery. In this suite, IP provides addressing, TCP provides connection-oriented message transmission, and User Datagram Protocol (UDP) provides connectionless, best-effort message transmission.

LearnTO: For additional information, check out LearnTO **Interpret IP Address** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

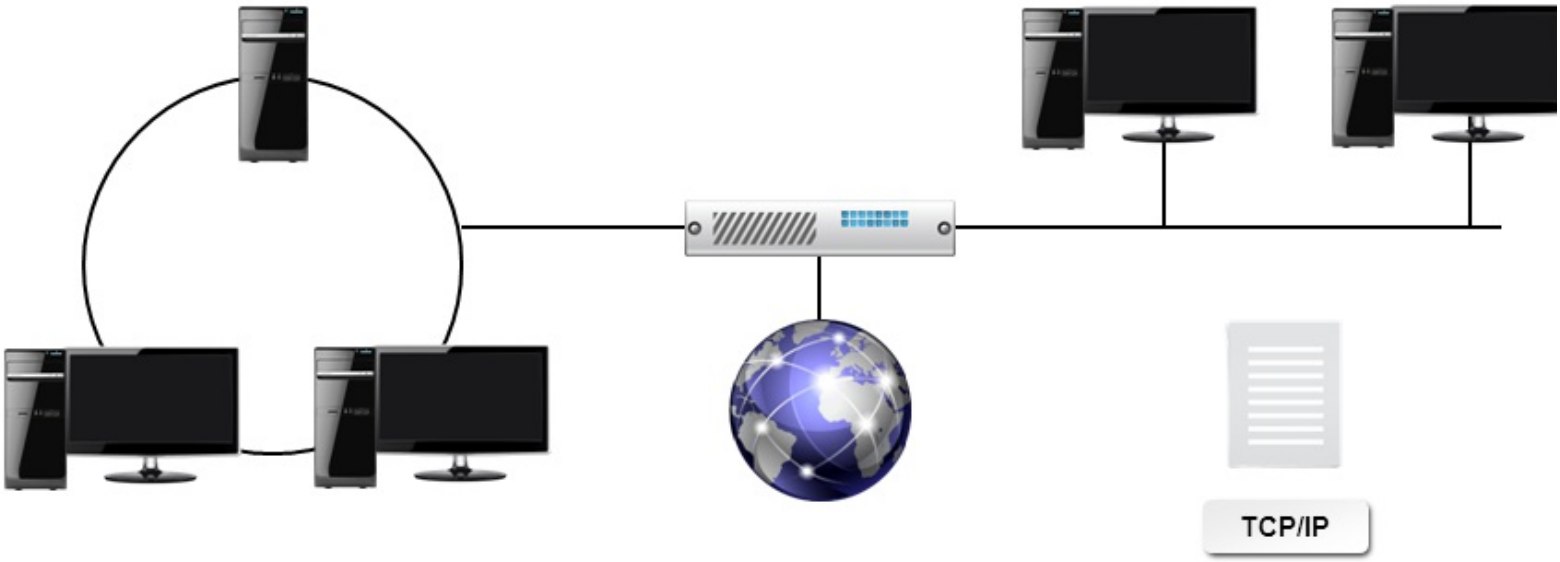


Figure: TCP/IP.

Nonproprietary, Routable Protocols

Nonproprietary means that no one group or organization owns or controls the protocol. You do not have to purchase software from a particular vendor or pay any kind of licensing fee to use TCP/IP.

Routable means the protocol can be used to communicate between different network sections. Thus, TCP/IP communications are not confined to a single network segment. To be routable, a protocol must provide addresses that identify individual network segments as well as network *hosts*.

Broadcast, Unicast, and Multicast

Broadcasts are network communications that are sent to all the computers on the network at once. Compare this to unicast transmissions, which are sent to a specific address or addresses, or multicast transmissions, which use a single address to transmit to a group of systems.

IPv4 Addresses

An *IPv4 address* is a 32-bit number assigned to a computer on a TCP/IP network. Some of the bits in the address represent the network segment; the other bits represent the computer, or node, itself. For readability, the 32-bit IPv4 address is usually separated by dots into four 8-bit octets, and each octet is converted to a single decimal value. Each decimal number can range from 0 to 255, but the first number cannot be 0. In addition, all four numbers in a host address cannot be 0 (0.0.0.0) or 255 (255.255.255.255).

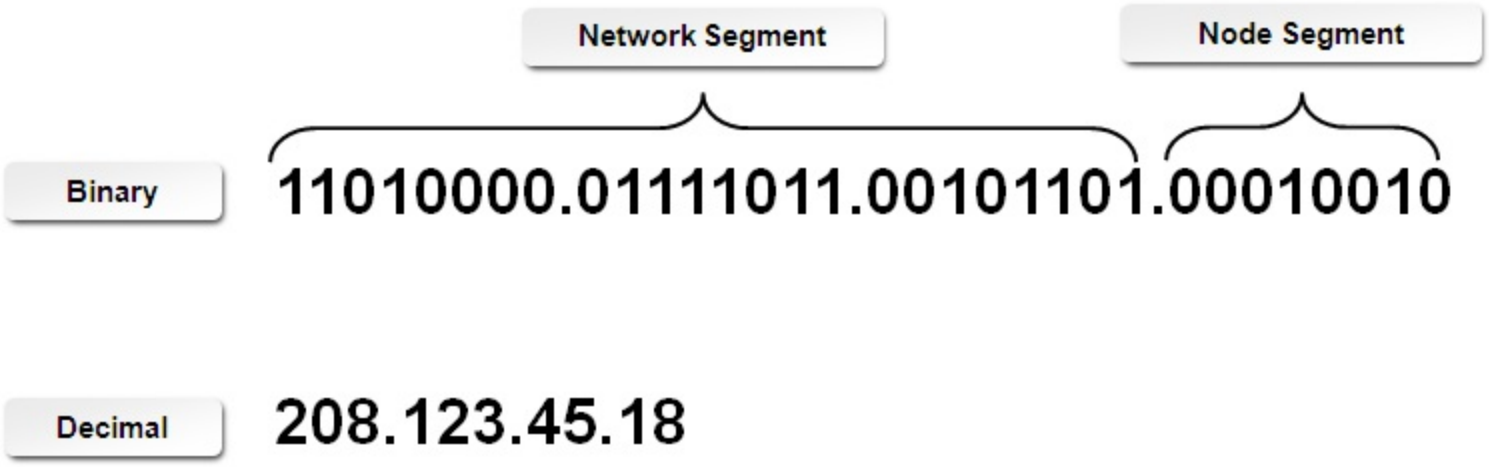


Figure: An IPv4 address.

Network Names

Systems on a network are typically assigned a host name, in addition to the numeric address. The host name is the descriptive name you see assigned to computers on the Internet, but systems on local networks have them as well. On the Internet, these host names appear to the left of the domain name. Host names can be up to 63 characters long.

Binary and Dotted Decimal Notation

TCP/IP uses binary numbering. Binary is a base 2 numbering system in which any bit in the number is either a zero or one. An IP address might appear in binary as 11001011.01111011.00101101.00010010.

Although the underlying IPv4 addresses are binary numbers, for readability, TCP/IP addresses are usually displayed in dotted decimal notation. Dotted decimal notation consists of four decimal numbers separated by three dots. Each decimal number is called an octet because it represents eight binary bits. When pronouncing a dotted decimal number, include the separator dots. For example, the IPv4 address 192.168.1.18 is pronounced one ninety-two dot one sixty-eight dot one dot eighteen.

Subnet Masks

A *subnet mask* is a 32-bit number that is assigned to each system to divide the 32-bit binary IP address into network and node portions. This makes TCP/IP routable. A subnet mask uses a binary operation to remove the node ID from the IP address, leaving just the network portion. Subnet masks use the value of eight 1s in binary, or 255 in decimal, to mask an entire octet of the IP address.

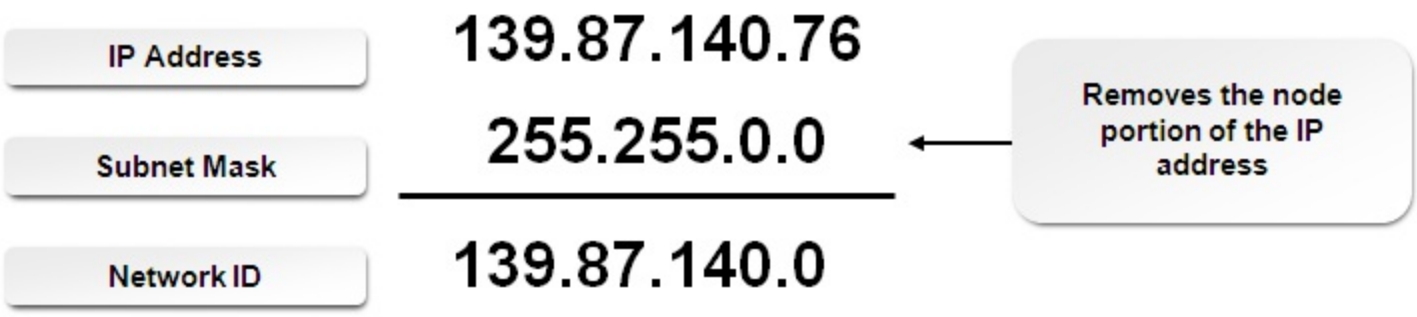


Figure: The subnet mask.

Binary ANDing

The binary logical operation applied to the subnet mask and the IP address is called binary ANDing. There are two rules in the binary AND operation:

- Zero AND any value equals zero.
- One AND one equals one.

To apply a subnet mask, you convert both the IP address and the subnet mask to binary. You AND each digit of the two binary numbers together. The zeros in the subnet mask convert all the bits in the node portion of the IP address to zeros, leaving the network portion of the address intact.

Gateways

A *gateway* is a device, software, or a system that has the ability to convert data between incompatible systems or devices. Gateways can translate data between different operating systems, or email formats, or between totally different networks. A gateway can be implemented as hardware, software, or both. You can also install gateways as software within a router, allowing the router to act as a gateway when required, and eliminating the need for separate hardware.

The Default Gateway

When TCP/IP communications need to be routed to systems on other networks, the protocol directs the packets to a special address known as the default gateway. The default gateway is different from a typical gateway in that the address is typically that of a network router that connects the local network to other external networks. A default gateway address is not a required component of a TCP/IP address assignment, but without a default gateway, the computer will only be able to communicate on the local network segment.

IP Address Classes

The designers of the TCP/IP suite defined five ranges of addresses, called address classes, for specific network uses and sizes. Changes in the Internet since the early 90s have rendered classful addresses all but obsolete. One of the final remnants of classful addressing is the use of the terms "Class A," "Class B," and "Class C" to describe common subnet masks.

Class and Subnet Mask	***Description***
Class A 255.0.0.0	*Class A* subnet masks provide a small number of network addresses for networks with a large number of nodes per network: • Number of nodes per network: 16,777,214 • Network ID portion: First octet • Node ID portion: Last three octets Used only by extremely large networks, Class A addresses are far too big for most companies. Large telephone companies and ISPs leased most Class A network addresses early in the development of the Internet.
Class B 255.255.0.0	*Class B* subnet masks offer a larger number of network addresses, each with fewer nodes per network: • Number of nodes per network: 65,534 • Network ID portion: First two octets • Node ID portion: Last two octets Most companies leased Class B addresses for use on Internet-connected networks. In the beginning, there were plenty of Class B addresses to go around, but soon they were depleted.
Class C 255.255.255.0	*Class C* subnet masks offer a large number of network addresses for networks with a small number of nodes per network: • Number of nodes per network: 254 • Network ID portion: First three octets

	• Node ID portion: Last octet Because there can be more Class C networks than any other type, they are the only addresses still generally available.

Classless Addressing

Because the traditional IP address classes have limitations on the number of available addresses in each class, there are now various implementations that utilize classless addressing. In these schemes, there is no strict dividing line between groups of addresses, and the network address/node address division is determined entirely by the number of 1 bits in the subnet mask.

IPv6 Addresses

IP version 6, or *IPv6,* is an Internet standard that increases the available pool of IP addresses by implementing a 128-bit binary address space. IPv6 also includes new efficiency features, such as simplified address headers, hierarchical addressing, support for time-sensitive network traffic, and a new structure for unicast addressing. One of the goals of IPv6 is to keep the IP headers as small as possible to make access to the address more efficient and quicker. Non-essential information in IPv6 headers is moved to optional extension headers. In IPv6, address blocks are automatically assigned hierarchically by routers. Top-level routers have top-level address blocks, which are automatically divided and assigned as routers and segments are added. This divides the address space logically instead of randomly, making it easier to manage.

IPv6 is not compatible with IPv4, so now, it is narrowly deployed on a limited number of test and production networks. Full adoption of the IPv6 standard will require a general conversion of IP routers to support interoperability. IPv6 makes use of an Institute of Electrical and Electronics Engineers (IEEE) standard called Extended Unique Identifier (EUI). A host computer implemented with EUI-64 can assign itself a 64-bit IPv6 interface identifier automatically.

Note: For more information on IPv6, see the IETF's IP Version 6 Working Group charter at **www.ietf.org/html.charters/ipv6-charter.html.**

The IPv6 Address Format

An *IPv6 address* has 128 bits or 16 bytes and is denoted as eight hexadecimal blocks separated by colons. The byte on the left has the highest order, and the byte on the right has the lowest order. To make the representation easier, some abbreviation techniques are used. For example, one abbreviation technique used replaces all zero hexadecimal values with a single zero and removes the leading and trailing zeros of all nonzero values.

For example, in the IPv6 address **2001:DB8:0000:0056:0000:ABCD:EF12:1234,** the third, fourth, and fifth bytes contain consecutive zeros and, therefore, they can also be represented as **2001:DB8:0:56:0:ABCD:EF12:1234** without the unnecessary zeros.

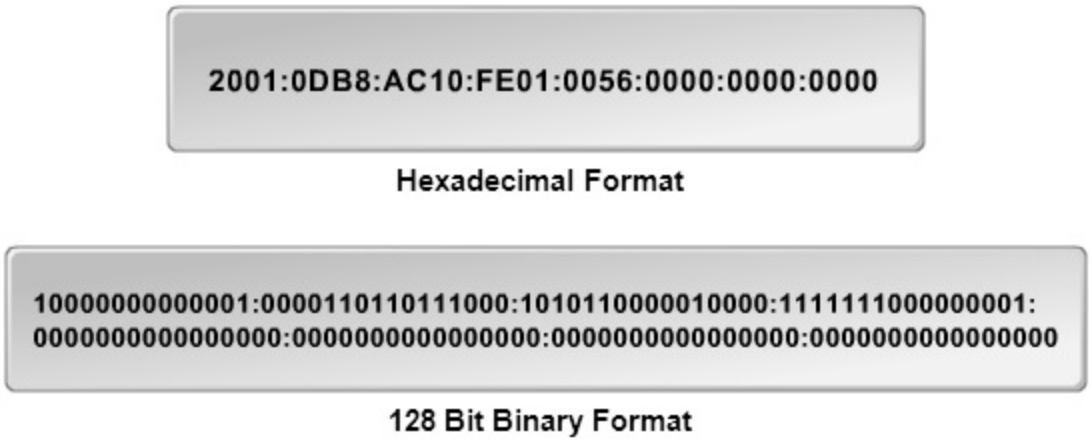


Figure: An IPv6 address.

Another technique used replaces all consecutive zero values or consecutive leading or trailing zeros with a double colon. However, the double colon can be used only once in an address. This is because when a computer comes across a simplified address, it replaces the double colon symbol with as many zeros as required to make it 128 bits long. If an address contains more than one double colon, the computer cannot determine the number of zeros for each place.

For example, the IPv6 address **2001:DB8:0000:0056:0000:ABCD:EF12:1234** can also be represented as **2001:DB8::56:0:ABCD:EF12:1234** or **2001:DB8:0:56::ABCD:EF12:1234** after replacing any one of the consecutive zeros with a double colon.

IPv4 vs. IPv6

IPv4 addresses use 32 bits as opposed to the 128 bits used in IPv6 addressing. While implementing IPv4 addresses, IPSec is optional. However, IPSec is not optional in IPv6 addresses. The header information structure is different between IPv4 and IPv6 addresses. IPv6 is not compatible with IPv4, so now, it is narrowly deployed on a limited number of test and production networks. Full adoption of the IPv6 standard will require a general conversion of IP routers to support interoperability.

Addressing Schemes

When assigning addresses to hosts on your network, you must assign an address in the right scheme based on the type of network and access is given to that host.

Scheme	*Description*
Private	*Private IP addresses* are addresses that organizations use for nodes requiring IP connectivity within enterprise networks, but not requiring external connections to the global Internet. IP addresses in each of the Classes A, B, and C are reserved as private IP addresses. When an Internet router receives a data packet bound for one of these reserved IP addresses, it recognizes the address as nonroutable and does not forward it outside the network. Private IP addresses can be used freely on internal networks. Because they are not routable, private IP addresses do not cause duplicate IP address conflicts on the Internet. Any organization that opts to use private IP addresses can do so without contacting the ICANN or an Internet registry. Because these addresses are never injected into the global Internet routing system, the address space can simultaneously be used by many different organizations. Problems arising due to the shortage of IP addresses are resolved by private IP addresses.
Public	*Public IP addresses* are addresses that get shared on the Internet. In order to keep internal addresses private, *Network Address Translation (NAT)* is used to conceal internal private IP addresses from external networks. A router is configured with a single public IP address on its external interface and a private address on its internal interface. A NAT service running on the router or on another system translates between the two addressing schemes. Packets sent to the Internet from internal hosts all appear as if they came from a single IP address, thus preventing external hosts from identifying and connecting directly to internal systems.
APIPA	*Automatic Private IP Addressing (APIPA)* is a feature of Windows that enables a Dynamic Host Configuration Protocol (DHCP) client computer to configure itself automatically with a random IP address in the range of 169.254.0.1 to 169.254.255.254 if there is no DHCP server available. APIPA enables DHCP clients to initialize TCP/IP and communicate with other local APIPA-configured machines, even in the absence of an active DHCP scope. APIPA addresses are not routable, so computers with APIPA addresses cannot communicate outside their local subnet. APIPA can be a useful configuration method on small home networks because computers can initialize TCP/IP and connect without any administrative configuration. On larger networks, however, a computer with an APIPA-range address is usually nothing more than a symptom, to the technician, of a DHCP problem that requires resolution.

Class Address Ranges

Each class of IP addresses is within a specific range of addresses.

Class	Starting IP Address	Ending IP Address
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255

Private Address Ranges

Each class of IP address has a reserved range for private IP addresses.

Class	Starting IP Address	Ending IP Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Loopback Address

Another reserved address is 127.0.0.1. It is referred to as the loopback or localhost address. It denotes "this computer." It is useful for testing services on a computer; anything sent to this address never leaves the computer as it loops back "home."

Static vs. Dynamic Addressing

On a TCP/IP network, you can assign IP address information statically to nodes by manually entering IP addressing information on each individual network node. Or, *dynamic addressing* can be used to assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) service.

Static addressing involves configuring TCP/IP statically on a network and requires that an administrator visit each node to manually enter IP address information for that node. If the node moves to a different subnet, the administrator must manually reconfigure the node's TCP/IP information for its new network location. In a large network, configuring TCP/IP statically on each node can be very time consuming and prone to errors that can potentially disrupt communication on the network. Static addresses are typically only assigned to systems with a dedicated functionality, such as router interfaces, network-attached printers, or servers that host applications on a network.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network service that provides automatic assignment of IP addresses and other TCP/IP configuration information on network systems that are configured as DHCP clients. DHCP requires a DHCP server computer configured with at least one active DHCP scope. The scope contains a range of IP addresses and a subnet mask, and can contain other options, such as a default gateway address or *Domain Name Server (DNS)* addresses. When the service is enabled, it automatically leases TCP/IP configuration information to DHCP clients for a defined lease period.

DNS

Computers on TCP/IP networks are assigned both a host name and an IP address. Users generally access systems by their descriptive names, and the network needs to translate, or resolve, those names into the relevant systems' IP addresses. The *Domain Name System (DNS)* is the primary name resolution service on the Internet as well as private IP networks.

DNS is a hierarchal system of databases that map computer names to their associated IP addresses. DNS servers store, maintain, and update the databases and respond to DNS client name resolution requests to translate host names to IP addresses. The DNS servers on the Internet work together to provide global name resolution for all Internet hosts. For example, the IP address 209.85.165.99 might map to **www.google.com.**

Hosts Files

Another way to resolve machine names to IP addresses is to provide each computer on the TCP/IP network with a hosts file. The hosts file is a text file that contains a list of computer names and their associated IP addresses. The use of hosts files predated the development of DNS and they are no longer commonly used, because this manual name-resolution method is practical only on very small and very stable networks. Adding a new computer, for example, requires that the hosts file of every computer that might need to reach it be manually updated with the new information.

However, a TCP/IP system will still use entries in the hosts file if the file is present, and the hosts file actually takes precedence over DNS name resolution. This can make the hosts file useful for testing purposes. However, if the hosts file is configured incorrectly, it can cause connectivity problems even when the DNS configuration is correct. Because altering the hosts file is a simple way to disrupt communications, the hosts file can be a target of attacks or malware. Be sure to check it when you troubleshoot name resolution and connectivity.

Client-Side DNS

Client-side DNS can be implemented by running a DNS service on a client computer. The client can quickly use the client resolver cache to lookup host names for resolution. This enables the client to perform basic DNS lookups without having to connect to a DNS server. In cases where the lookup is out of scope for the client resolver, the DNS servers that store, maintain, and update databases will respond to any resolution requests that may be out of scope for client-side DNS services to handle. In this case, the client-side DNS service will communicate directly with multiple DNS servers to resolve name requests made from the client machine.

ACTIVITY 6-2: Identifying Your Computer's TCP/IP Information

Scenario

In this activity, you will examine the configuration settings on your computer that enables it to connect to the network.

1. Determine the protocol in use on your system.
   a. Select **Start→Control Panel.** In the **Search Control Panel** text box, type ***network connections***
   b. Under **Network and Sharing Center,** select **View network connections.**
   c. Examine the contents of the **Network Connections** window. One of the connections that is displayed in this window is the connection to the class network.
   d. Display the pop-up menu for the network connection, and select **Properties.**
   e. In the **This connection uses the following items** list, verify that **Internet Protocol Version 4 (TCP/IPv4)** is listed.
   f. Close the **Properties** dialog box without making any changes.
2. View the TCP/IP information assigned to your network adapter.
   a. Display the pop-up menu for the network connection, and select **Status.**
   b. Select **Details.**
   c. In the **Network Connection Details** dialog box, examine the information for the IPv4 address, subnet mask, and default gateway.
3. In the **Network Connection Details** dialog box, examine the information for DHCP.

4. **If DHCP is enabled on your computer, when does the lease expire?**

   A: Answers will vary depending on the last time the computer was restarted.

5. In the **Network Connection Details** dialog box, examine the information for DNS.

6. **How many DNS servers are listed?**

   A: Answers will vary depending on the configuration of the network.

7. Return to the network connection properties, and examine the **Internet Protocol Version 4 (TCP/IPv4)** properties.
   a. Select **Close.**
   b. Select **Properties** to return to the network connection properties.
   c. In the **This connection uses the following items** list, select **Internet Protocol Version 4 (TCP/IPv4),** and then select **Properties.**
   d. Select **Advanced.**
   e. Select the **DNS** tab.

f. Select **Cancel** three times, and then select **Close.**
g. Close the **Network Connections** window.

Topic C: Network Connectivity

In the previous topics, you identified network communication technologies and the components of TCP/IP. To complete your understanding of network concepts, you will need to examine the technologies that connect multiple nodes and networks together. In this topic, you will identify network connectivity technologies.

Putting together a network is like putting together a huge puzzle. There are physical pieces, such as network adapters and network clients, and conceptual pieces, such as protocols and addresses. To understand how the pieces all fit together, however, you need to be able to see the overall picture. Examining the large structures and techniques that provide network connectivity between and within network locations will help you see the big picture of network implementation and support.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 2.7: Compare and contrast Internet connection types and features.
- Objective 2.8: Identify various types of networks.
- Objective 2.9: Compare and contrast network devices, their functions, and features.

LANs

A *Local Area Network (LAN)* is a self-contained network that spans a small area, such as a single building, floor, or room. In a LAN, all parts of the network are directly connected with cables or short-range wireless media.

Figure: LANs within a building.

WANs

A *Wide Area Network (WAN)* is a network that spans multiple geographic locations. WANs typically connect multiple LANs using long-range transmission media. Such a network scheme facilitates communication among users and computers in different locations. WANs can be private, such as those built and maintained by large, multinational corporations, or they can be public, such as the Internet.

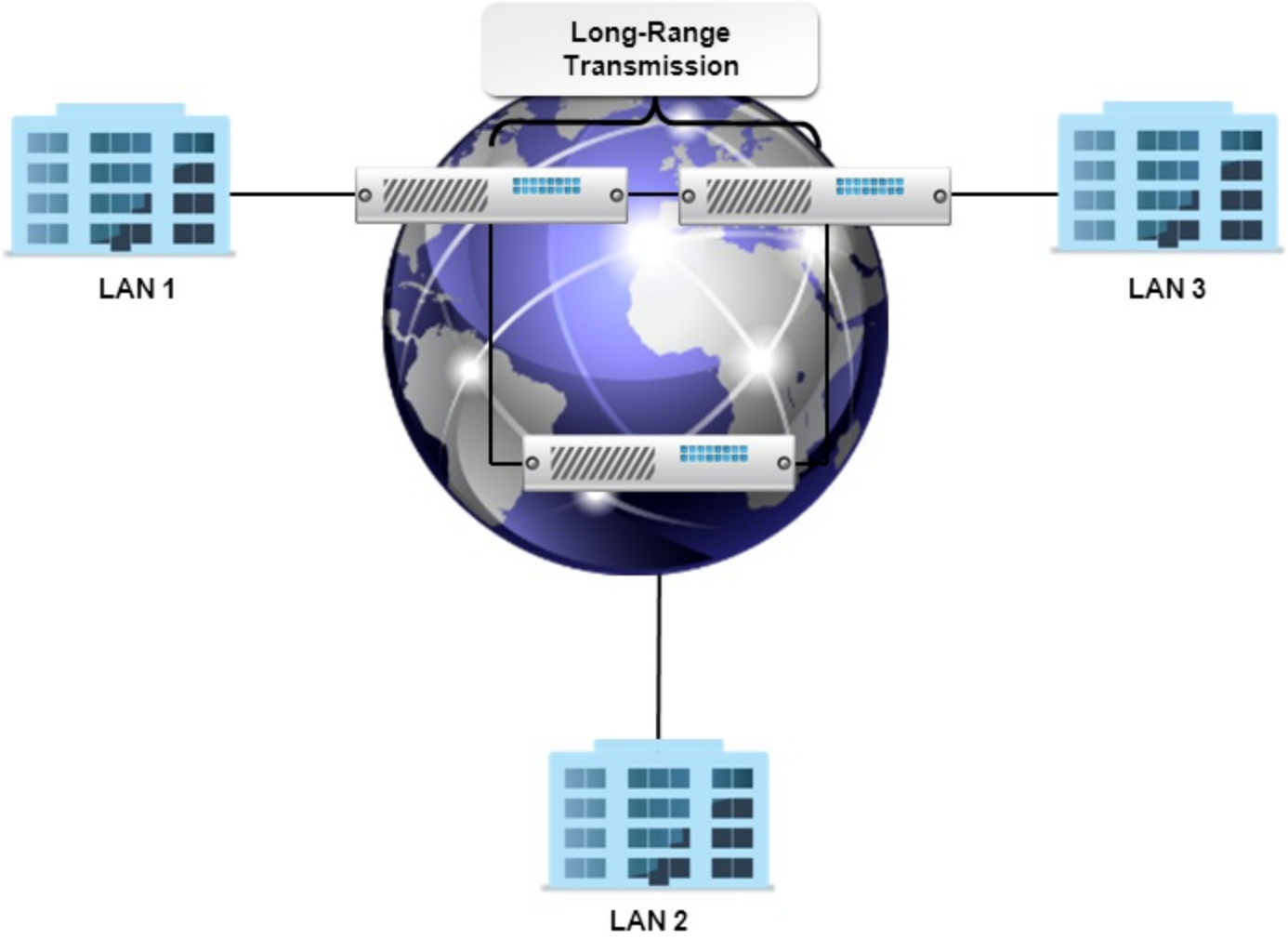


Figure: A WAN.

PANs

A *Personal Area Network (PAN)* connects two to three devices together for use by one person using a router with cabling; most often seen in small or home offices.

A *Wireless Personal Area Network (WPAN)* is a network that connects wireless devices in very close proximity but not through a Wireless Access Point (WAP). Infrared and Bluetooth are some technologies used for connecting devices in a WPAN.

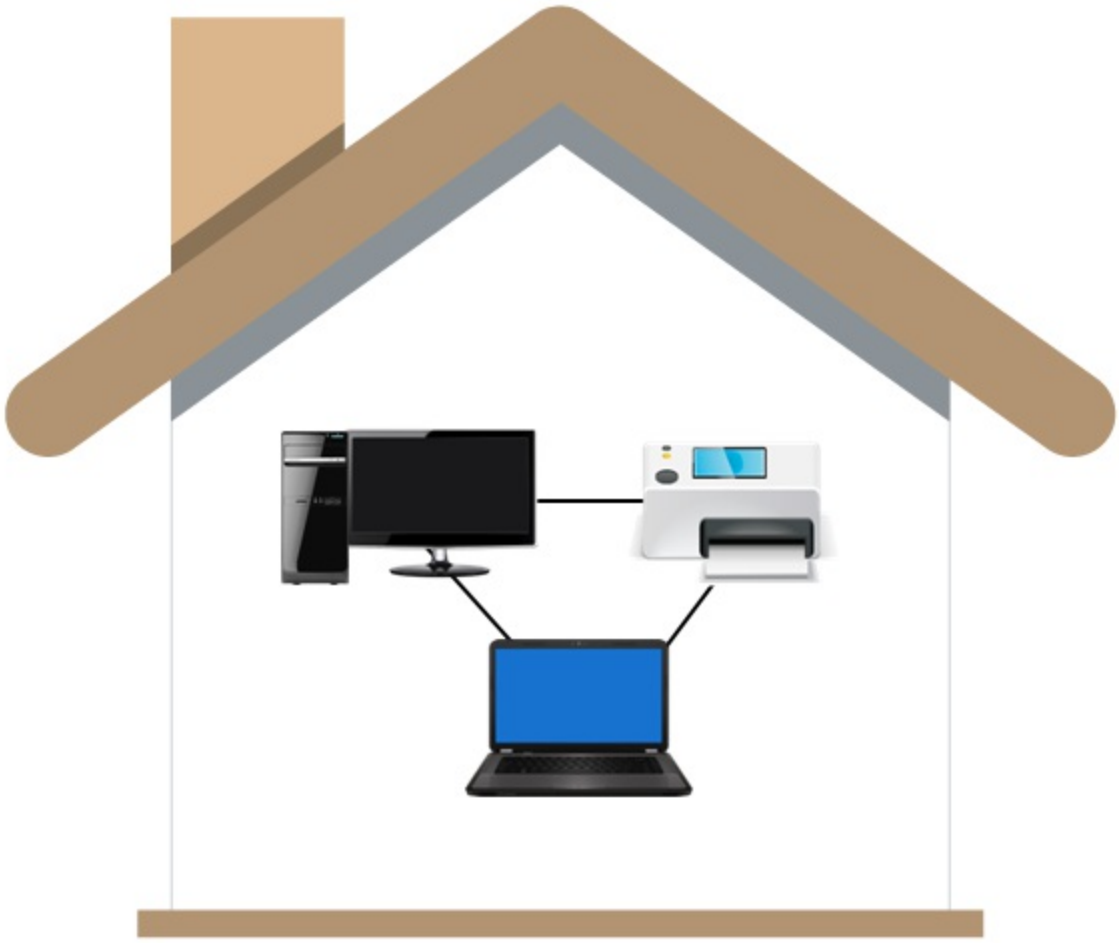


Figure: A PAN.

MANs

A *metropolitan area network (MAN)* covers an area equivalent to a city or other municipality. In many cases the MAN connects multiple LANS.

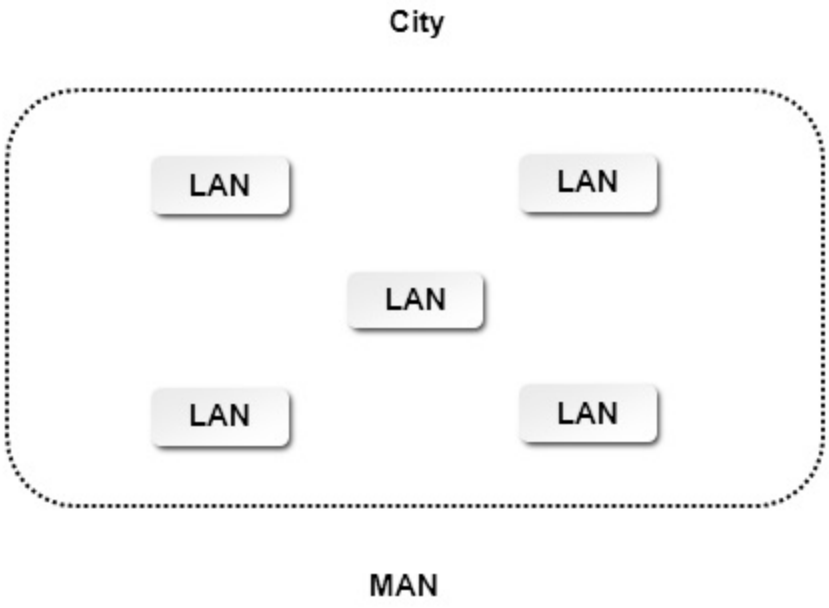


Figure: A MAN.

Additional Network Types

While on the job, you may come across several other loosely defined network categories, named according to the geographic areas they cover. These include:

- A *campus area network (CAN),* which covers an area equivalent to an academic campus or business park. A CAN is typically owned or used exclusively by one company, school, or organization.
- A *global area network (GAN),* which is any worldwide network.

VPNs

A *virtual private network (VPN)* is a private network that protects communications sent through a public network, such as the Internet. VPNs provide secure connections between endpoints, such as routers, clients, or servers, by using tunneling to encrypt data. These connections are established either between two LANs or between a user and a LAN over the Internet. Special *VPN protocols* are required to provide the VPN *tunneling,* security, and data encryption services.

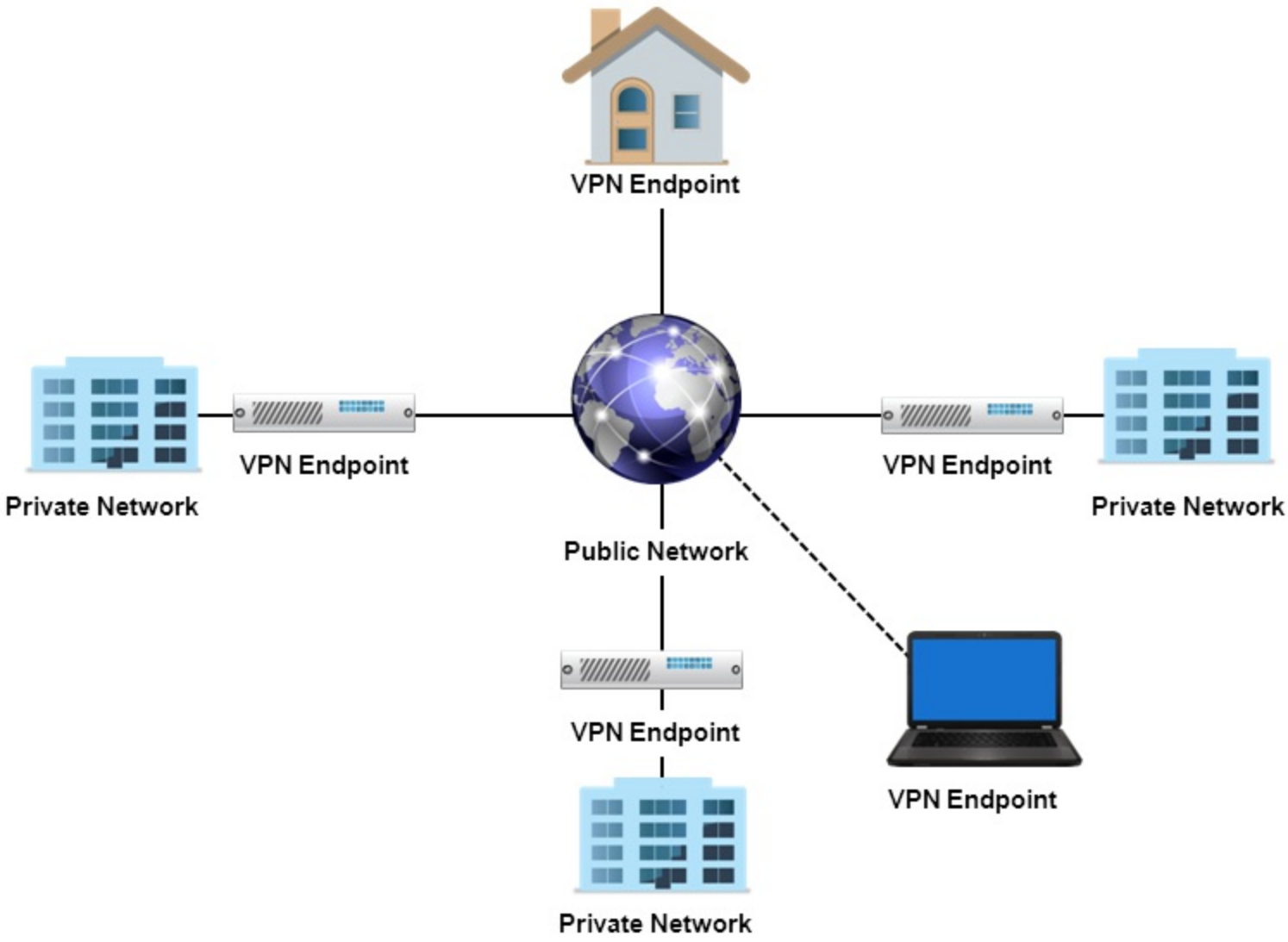


Figure: A VPN.

Ethernet

An *Ethernet* network is a popular LAN implementation that uses Ethernet network adapters, contention-based media access, and twisted pair, coax, or fiber media. Xerox® corporation first developed Ethernet in the 1970s. Later, the IEEE used Ethernet as the basis of the 802.3 specification, which standardized Ethernet and expanded it to include a wide range of cable media. The 802.3 family of specifications also determines transmission speed (10 Mbps, 100 Mbps, or 1000 Mbps) and signal method (baseband or broadband).

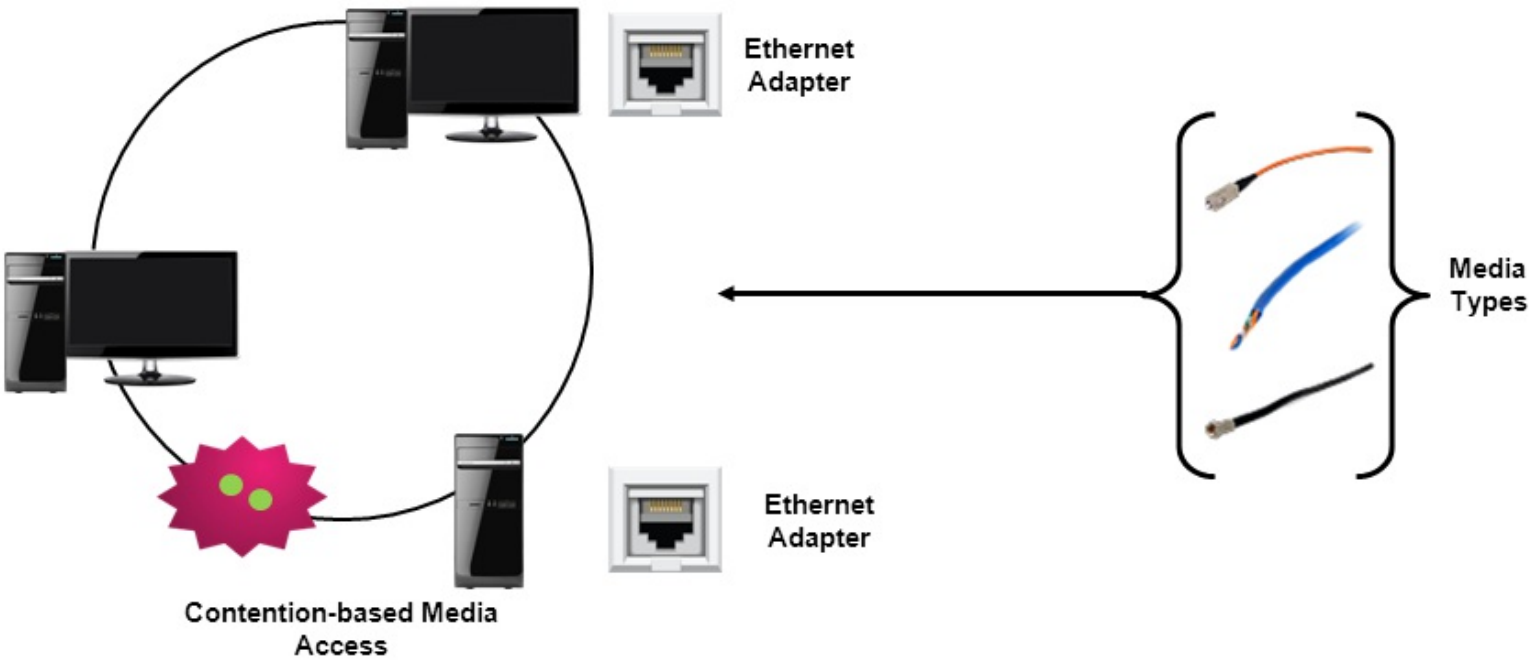


Figure: Ethernet.

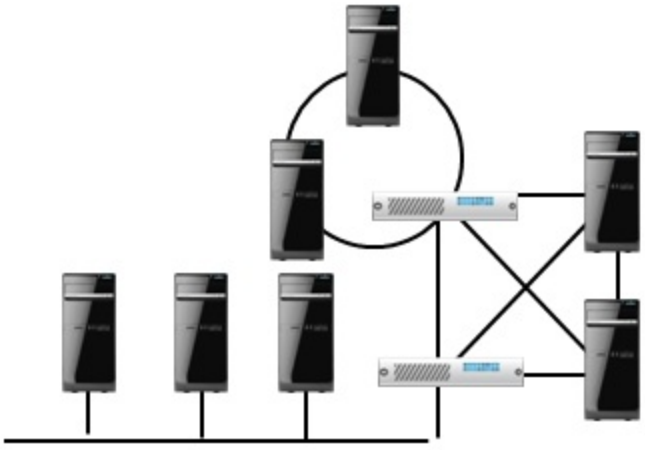
Ethernet WAN

To implement an Ethernet WAN, in most cases, you establish a connection to the Internet by using Ethernet technology on the LAN and a broadband Internet connection such as a cable modem or digital subscriber line (DSL) modem. After you connect to the Internet, you can then connect to your organization's LAN using a VPN. Use Ethernet WANs when you want to enable users to connect remotely to the Internet, your company's VPN, or both.

Network Topologies

A *network topology* is a specification that determines the network's overall physical layout and transmission and flow patterns. There are a number of different topologies used to configure networks.

Topology	*Description*
Mesh	A *mesh topology* is a network topology in which each node is directly connected to every other node, similar to the physical point-to-point topology. This configuration allows each node to communicate with multiple nodes at the same time. Since all nodes have dedicated links with other nodes, there is no congestion on the network and data travels very fast. Since no node can be isolated from the network, this topology is extremely reliable. It is also difficult to implement and maintain because the number of connections increases exponentially with the number of nodes. Mesh topologies typically provide reliable connections between separate independent networks.
Ring	A *ring topology* is a network topology in which each node is connected to the two nearest nodes: the upstream and downstream neighbors. The flow of data in a ring network is unidirectional to avoid collisions. All nodes in the network are connected to form a circle. There is no centralized node to control network traffic and each node handles every data packet that passes through it. Data transmission moves in one direction to each node that scans data packets, accepts packets destined for it, and forwards packets destined for another node.
	A *bus topology* is a network topology in which nodes receive the data transmitted all at the same time, regardless of the physical wiring layout of the network. Data flow propagates in a single, continuous stream.

Bus	
Star	A *star topology* is a network topology that uses a central connectivity device, such as a hub or a switch, with individual physical connections to each node. The individual nodes send data to the connectivity device, and the device then either forwards data to the appropriate destination node, as in the case of a switch, or simply passes it through to all attached nodes, as in the case of a hub. Star topologies are reliable and easy to maintain as a single failed node does not bring down the whole network. However, if the central connectivity device fails, all nodes on that device fail to communicate.
Hybrid	A *hybrid topology* is any topology that exhibits the characteristics of more than one standard topology. Each section of the network follows the rules of its own topology. They can be complex to maintain because they typically incorporate a wide range of technologies. Most of the large networks consist of several smaller subnetworks, and each subnetwork may have a different topology. 

Network Device Types and Features

Computers attached to a network need to have their data mediated by a network device, and there are several kinds of network devices.

Network Device	*Description*
Hub	A *hub* is a device that connects multiple Ethernet or twisted pair devices together. By this connection, multiple devices can act as a single network segment. Hubs can either simply receive data transmitted from a device on one port and broadcast it out to the devices connected on all other ports, or they can perform the same receive-then-broadcast action but regenerate or boost the signal. Hubs are generally inexpensive and easy to manage; however, they do not provide the best performance in high-traffic or latency-sensitive situations. Hubs have largely been replaced by switches, but many dedicated hubs still remain in use. Troubleshooting a hub is made easier by the use of status lights for the various ports.
Switch	A *switch* is a network hardware device that joins multiple computers together within the same LAN. Unlike a hub, switches forward packets to only the destination port based on MAC addresses. Because of this, they are slightly "smarter" than hubs, and are more common. Switches can also be connected to other switches, thus increasing the number of devices on a LAN without sacrificing performance. Troubleshooting a switch is made easier by the use of status indicator lights on the various ports.
Router	A *router* is a networking device that connects multiple networks that use the same protocols. Traffic from one network to another does not always have to travel between the same routers. On the Internet, for example, traffic is routed according to the best available path at the time. Troubleshooting a router is made easier by the use of status indicator lights on the various ports.
Bridge	A *bridge* is a network device that divides a logical bus network into segments. Bridges examine the MAC address of each packet. If the packet is destined for a node connected to a different port, the bridge forwards the packet. If the packet is addressed to a node on its own segment, the bridge does not forward the packet. This arrangement reduces traffic between segments and improves overall network performance.
Access Point	An *access point (AP)* is a device or software that facilitates communication and provides enhanced security to wireless devices. It also extends the physical range of a WLAN. The AP functions as a bridge between wireless STAs (stations) and the existing network backbone for network access.
Modem	A *modem* is a device that modulates and demodulates digital data to an analog signal that can be sent over a telephone line. Its name is a combination of *mo*dulate and *dem*odulate. Use a modem to connect to the Internet and to translate digital information to and from your computer. Depending on the type of connection used, you will use either a cable modem, a

	DSL modem, a wireless modem, a voice modem, or a radio modem. A laptop modem can be an internal device, or can be added to a system using a PC Card or an ExpressCard.
NAS	A *network-attached storage (NAS)* appliance is a data storage device that can be connected to a network to provide direct data access and file sharing to multiple computing devices attached to the network.
Firewall	A firewall is a software program or hardware device that protects networks from unauthorized data by blocking unsolicited traffic. Firewalls allow incoming or outgoing traffic that has specifically been permitted by a system administrator and incoming traffic that is sent in response to requests from internal systems. Firewalls use complex filtering algorithms that analyze incoming network data based on destination and source addresses, port numbers, and data type.
VoIP phones	*Voice over IP (VoIP)* phones can transmit voice signals over IP data networks. With VoIP, the phone system and IP network translate between voice and network signals and between phone numbers and IP addresses. You can make a telephone call and the signal will be transmitted over your network connection and transferred to the standard phone system if the called party does not have VoIP service. Conversely, when a caller dials a phone number that maps to a VoIP device, VoIP routes the call to the IP host.
Internet appliance	An *Internet appliance* is a device that allows quick easy access to the Internet. It can be connected to a number of computing devices for allowing access to Internet services.

ISPs

An *Internet Service Provider (ISP)* is a company that provides Internet access to individuals and to businesses. Most ISPs charge a fee for this connection. Customers receive logon information, access to servers that provide name resolution and email services, dynamic or static IP configurations, and a method for connecting to the ISP. Once connected to the ISP, the customer can access the Internet.

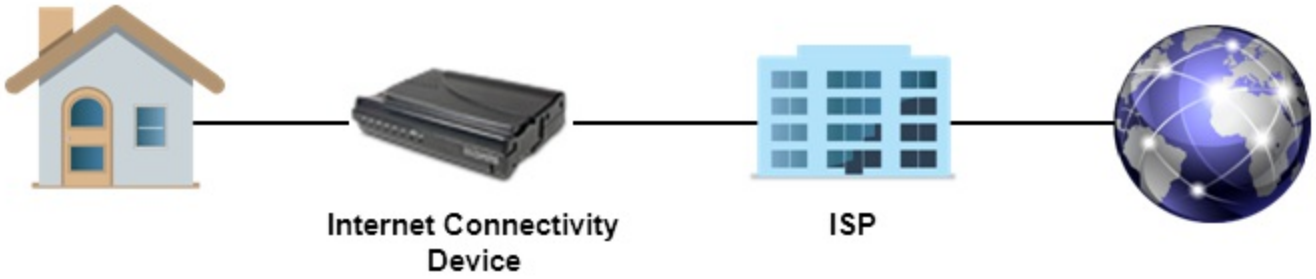


Figure: An ISP.

Broadband Communications

Broadband is a general term for a category of network transmission technologies that provide high throughput by splitting communications into multiple channels transmitted simultaneously over the network media. Today's common broadband network communications technologies are typically employed to provide affordable high-speed Internet access to homes and businesses.

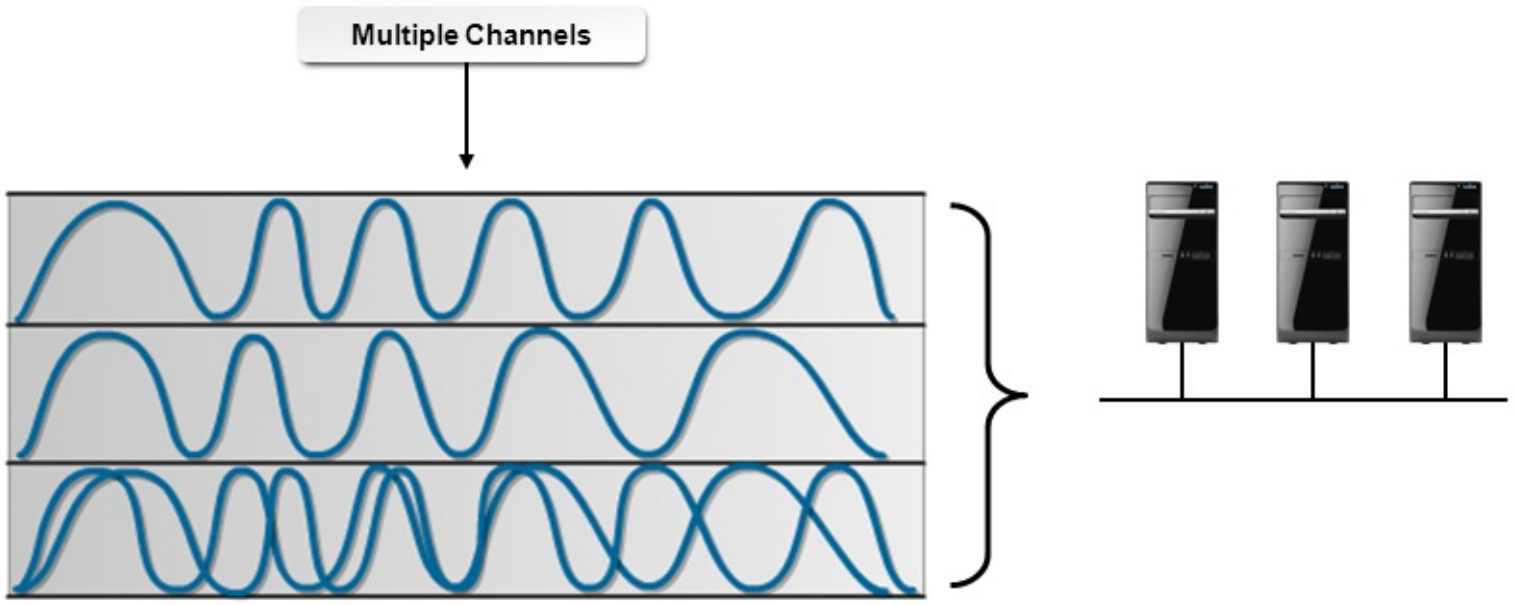


Figure: Broadband transmission.

Baseband vs. Broadband

The opposite of broadband is *baseband.* In baseband transmissions, a single signal sends data using the entire bandwidth of the transmission media. Devices cannot simultaneously send and receive data.

Neither baseband nor broadband is inherently faster or slower, but broadband is effectively faster on large public networks, notably the Internet, where multiple clients are trying to send and receive data simultaneously. For this reason, in common usage, broadband networks have become synonymous with fast networks, although not all fast networks use broadband signaling. There is no single common definition of the minimum data rate for a technology to be fast enough to qualify as broadband in this sense, although a one-way transmission rate in the range of at least 1.5 Mbps is typical.

Internet Connection Types and Features

Internet connections can be accomplished in a wide variety of ways today. Each method has unique connection technology that is used to connect computing devices to the Internet.

Method	*Description*
Cable	*Cable* or *cable modem* transmissions use a cable television connection and a specialized interface device known as a cable modem to provide high-speed Internet access to homes and small businesses. Cable access arranges users in groups around nodes that split the television and data signals at the cable provider's end. The speed of the network varies depending on how populated the group on each node is. Download speeds can vary by more than 1 Mbps in different areas. Most cable companies try to guarantee at least a 768-Kbps download speed; however, speeds of 3.0 to 7.0 Mbps are common, and speeds of 20 Mbps or more are possible.
DSL	*Digital Subscriber Line (DSL)* is a broadband technology that transmits digital signals over existing phone lines. It has become a popular way to connect small businesses and households to the Internet because it is affordable and provides a relatively high download speed—a typical maximum is 1.5 Mbps for basic DSL and 7 Mbps for high-end DSL. However, distance from the phone company's switching station and the quality of the lines affect the total bandwidth available to a customer.
Dial-up	*Dial-up lines* are local loop *Public Switched Telephone Network (PSTN)* connections that use modems, existing phone lines, and existing long-distance carrier services to provide low cost, low bandwidth WAN connectivity, and remote network access. Dial-up lines are generally limited to 56 Kbps, and are sometimes used as backups for higher bandwidth WAN services.
Fiber	*Fiber* is a method used to connect devices to the Internet using fiber optic cable. Fiber is mostly used in smaller areas to connect computing devices to a router. It provides a fast data exchange rate over distances of several kilometers.
Satellite	Orbiting *satellites* provide extremely long-range wireless network transmissions. For broadband network access, satellites can be employed to relay network signals from the network service provider to individual customers. This can be a way to provide broadband network communications in rural or remote areas where cable service or viable DSL lines are not available. However, satellite Internet communications are comparatively expensive and some only operate one-way; satellite transmissions provide the downstream communication, but another media (typically telephone) is needed for upstream communication. For remote or mobile locations, true two-way satellite-only communication is also available, but aligning a dish for upstream communication to a satellite requires a certain degree of precision and skill.
	Integrated Services Digital Network (ISDN) is a digital transmission technology that carries both voice and data over digital phone lines or PSTN wires. Connections are made

ISDN	on demand by dialing another ISDN circuit's telephone number. ISDN and DSL are very similar technologies because they both use existing phone lines to transmit digital signals. However, ISDN technology predates DSL and has largely been superseded by DSL for the home and small business market. ISDN requires a specialized client adapter called a Terminal Adapter, which DSL does not. ISDN is also slower than DSL, being limited to a data rate of approximately 128 Kbps for basic rate ISDN, and thus barely qualifies as broadband. (Primary rate ISDN, which was commonly used for network backbone communications before fiber optic cable, provides more bandwidth and has higher speeds.)
Cellular	*Cellular* technology uses radio signals to transmit network data over the cellular telephone system. Cellular-enabled computers have a cellular radio built in. Coverage can be regional, national, or global, depending on the service chosen and the capabilities of the cellular service provider. Signal fidelity will vary depending on interference and the distance from a cell tower. Some of the cellular transmission technologies and standards in use include Code-Division Multiple Access (CDMA) and the Global System for Mobile Communications (GSM). CDMA is a spread-spectrum implementation that uses the full frequency spectrum for each channel rather than assigning specific frequencies to particular users. It separates the calls using digital encoding. GSM uses time-division multiplexing (TDM), which transmits multiple calls on the same frequency by dividing each call into separate time slices. Use a cellular *Wireless WAN (WWAN)* when you have users that have no other way to connect to the Internet, your company's VPN, or both. Cellular WWANs are typically more expensive than Ethernet WANs.
WiMAX	*Wireless Interoperability for Microwave Access (WiMAX)* is a packet-based wireless telecommunication technology that provides wireless broadband access over long distances. Based on the *IEEE 802.16* standard, it is intended for wireless MANs. WiMAX provides fixed as well as mobile broadband access. It covers a range of about 30 miles for fixed stations and 3 to 10 miles for mobile stations. WiMAX also provides line of sight and non-line-of-sight communication, and can provide connection speeds of about 70 Mbps. WiMAX operates in the wireless frequency ranges of between 2 and 11 GHz of the wireless spectrum. Line of sight communication is a method used when distances between devices can be seen by the human eye. In wireless networking this term can be used to determine whether an access point is within a certain distance and is within an acceptable range of connecting devices. There are a few terms used when referring to line of sight factors: • *Line-Of-Sight (LOS):* Wireless signals that travel over a direct visual path from a transmitter to a receiver.

	• *Non-Line-Of-Sight (NLOS):* Wireless signals that reach a receiver through reflections and obstructions within the visual path in the environment.
Bluetooth	Bluetooth® is a wireless radio protocol that is used to communicate from one device to another in a small area, usually less than 30 feet. Bluetooth is commonly used to enable communication between small personal electronic devices, such as between a cellular phone and a wireless earpiece or between an electronic organizer and a personal computer. Bluetooth uses the 2.4 GHz spectrum to communicate a 1 Mbps connection between two devices for both a 232 Kbps voice channel and a 768 Kbps data channel (technically, Bluetooth detects other devices in the 2.4 GHz spectrum and avoids the frequencies they use by "hopping" to an available frequency). Bluetooth 2.0 is an improved version of Bluetooth, has a range up to 100 meters, offers faster data transfer speeds (up to 3 Mbps), and also uses less power to extend battery life. Bluetooth 2.0 is backwards-compatible with earlier versions of Bluetooth, but the connection between devices is governed by the slowest device; in other words, connecting a Bluetooth 1.2 device to a Bluetooth 2.0 device means the data transfer is at the rate of Bluetooth 1.2. Bluetooth 3.0 is available but not yet widely adopted, though it boasts speeds up to 24 Mbps.

Bluetooth Naming and Addressing

Each Bluetooth device has its own unique 48-bit address. But instead of requiring you to connect via this address, most Bluetooth devices also have their own Bluetooth names. By default, manufacturers set the Bluetooth name for devices to the name of the manufacturer and model of the device. If you have several users you support that are in close proximity to each other and have the same devices, these default Bluetooth names can cause problems. In this scenario, you should be sure to rename each user's Bluetooth device.

Bluetooth Pairs

Most Bluetooth devices require you to establish a trusted relationship between two devices (referred to as pairing). This trusted relationship is established through the use of an encrypted shared secret or passkey. After the relationship is established, the pair of devices can encrypt the data transmissions they exchange. However, most Bluetooth printers permit all devices to use their services without requiring pairing.

ACTIVITY 6-3: Discussing Network Connectivity

Scenario

In this activity, you will discuss network connectivity.

1. **The transmission method that allows multiple signals to be carried separately on the same media at the same time is called _____**

   __ Baseband.
   _x_ Broadband.
   __ Modulated.
   __ Multicast.

2. **Which broadband communication method uses existing telephone lines to transmit digital signals?**

   __ Cable modem
   _x_ DSL
   __ ISDN
   __ Fiber
   __ Satellite

3. **Which broadband communication method uses the same physical media to provide high-speed transmission of data and television signals?**

   _x_ Cable modem
   __ DSL
   __ ISDN
   __ Fiber
   __ Satellite

4. **Which broadband communication method uses light to carry signals?**

   __ Cable modem
   __ DSL
   __ ISDN
   _x_ Fiber
   __ Satellite

5. **Which are wired connection technologies?**

__ Bluetooth
_x_ ISDN
_x_ Dial-up connections
__ Wi-Fi

6. **Which are wireless connection technologies?**

_x_ Bluetooth
__ Fiber optic
_x_ Cellular WAN
__ Twisted-pair

7. **Which wireless technology provides broadband Internet coverage in rural or remote areas?**

__ Cellular WAN
_x_ Satellite
__ Wi-Fi
__ Infrared
__ Bluetooth

8. **Which wireless technology is a short-range connection method requiring direct line of sight?**

__ Cellular WAN
__ Satellite
__ Wi-Fi
_x_ Infrared
__ Bluetooth

9. **When would some of the different Internet connection types be used and when do you think you might encounter them within the workplace?**

A: Answers will vary depending on the physical location and the needs of the organization, but might include wireless connectivity for a workplace that has a lot of laptops deployed.

10. **If you have remote employees that need to connect to the corporate network but they are located in a remote area with no access to broadband Internet service, what do you think is the best Internet connection method to use in this situation?**

A: Answers will vary, but will most likely include using either dial-up or satellite. However, because this employee needs to access the corporate network through a VPN connection, satellite will probably provide the faster connection. In some cases, tethering to a cell phone or connecting to a wireless network device is an option, but this will all depend on how remote the employee's location is and whether they can get a strong cellular signal.

Topic D: Ports and Protocols

In the previous topic, you explored the different network types and how they are connected. Now that you have a good understanding of how a network can be structured physically, you are ready to examine the various ports and protocols that are used to ensure data transmission is successful and secure. In this topic, you will examine common TCP and UDP ports and protocols.

Properly configuring the ports of a network device and selecting the right protocol will ensure that data gets transmitted over the network. As an A+ technician, you must understand how ports and protocols are implemented within a network and how they function to provide the right level of data transmission while keeping data secure.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 2.4: Explain common TCP and UPD ports, protocols, and their purpose.

Ports

In TCP/IP networks, a *port* is the endpoint of a logical connection. Client computers connect to specific server programs through a designated port. All ports are assigned a number in a range from 0 to 65,535. An international agency, the Internet Assigned Numbers Authority (IANA), separates port numbers into three blocks: well-known ports, which are preassigned to system processes by the IANA; registered ports, which are available to user processes and are listed as a convenience by the IANA; and dynamic ports, which are assigned by a client operating system as needed when there is a request for service.

TCP vs. UDP

The TCP/IP protocol suite includes two Transport-layer protocols: *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)*. TCP is a connection-oriented, guaranteed-delivery protocol used to send data packets between computers over a network such as the Internet. It is part of the Internet protocol suite along with the *Internet Protocol (IP)*. TCP is responsible for breaking up data into datagrams, reassembling them at the other end, resending data lost in transit, and resequencing data. It sends data, waits for an acknowledgement, and fixes erroneous data. IP is responsible for routing individual datagrams and addressing.

The User Datagram Protocol (UDP), also known as the Universal Datagram Protocol, is a connectionless Transport-layer protocol in the Internet protocol suite. A connectionless, best-effort delivery protocol, UDP is used with IP like TCP. It transmits data and ensures data integrity as TCP does. UDP, however, lacks reliability, flow-control, and error-recovery functions. It is less complex than TCP, and since it is a connectionless protocol, it provides faster service.

Port Ranges

There are three recognized blocks of port numbers.

Block	*Range*	*Description*
Well-known ports	Port range: 0 to 1,023.	Well-known ports are pre-assigned for use by common, or well-known, services. Often the services that run on these ports must be started by a privileged user. Services in this range include HTTP on TCP port 80, IMAP on TCP port 143, and DNS on UDP port 53.
Registered ports	Port range: 1,024 to 49,151.	These ports are registered by software makers for use by specific applications and services that are not as well known as the services in the well-known range. Services in the registered port range include SOCKS proxy on TCP port 1080, QuickTime® Streaming Server administration on TCP port 1220, and Xbox® Live on TCP and UDP port 3074.
Dynamic or private ports	Port range: 49,152 to 65,535.	These ports are set aside for use by unregistered services and by services needing a temporary connection.

Common Ports

This table lists some of the most common well-known TCP and UDP port numbers. Additional well-known ports and other port number assignments are available online at **www.iana.org/assignments/port-numbers.**

Port	*Type*	*Service Name*	*Purpose*
21	TCP	FTP	File transfers
22	TCP/UDP	SSH	Secure shell for secure data transmission
23	TCP/UDP	TELNET	Telnet services
25	TCP	SMTP	Simple mail transfers
53	TCP/UDP	DNS	Domain name system
80	TCP	HTTP	Hypertext transfer protocol
110	TCP	POP3	Post office protocol
143	TCP/UDP	IMAP	Internet message access protocol
443	TCP	HTTPS	HTTP secure combines HTTP with SSL/TLS protocols.
3389	TCP/UDP	RDP	Remote desktop protocol

LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol that defines how a client can access information, perform operations, and share directory data on a directory server. It was designed for use specifically over TCP/IP networks and on the Internet in particular. In most implementations, LDAP relies on the DNS service. First, DNS enables clients to find the servers that host the LDAP directory, and then the LDAP servers enable clients to find directory objects. Most common network directories are LDAP-compliant.

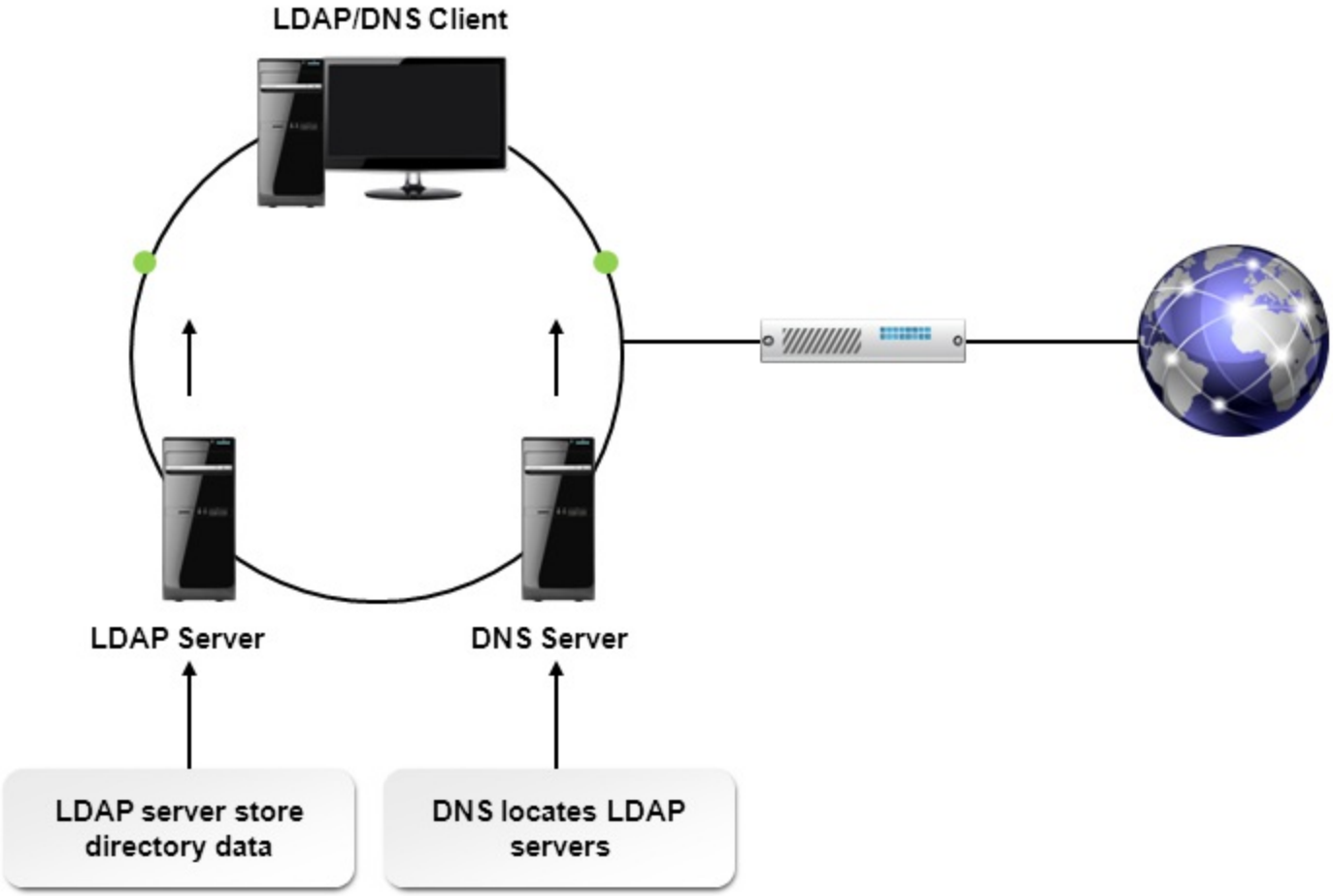


Figure: LDAP.

SNMP

Simple Network Management Protocol (SNMP) is an Application-layer protocol used to collect information from network devices for diagnostic and maintenance purposes. SNMP includes two components: management systems and agent software, which are installed on network devices such as servers, routers, and printers. The agents send information to an SNMP manager. The SNMP manager can then notify an administrator of problems, run a corrective program or script, store the information for later review, or query the agent about a specific network device.

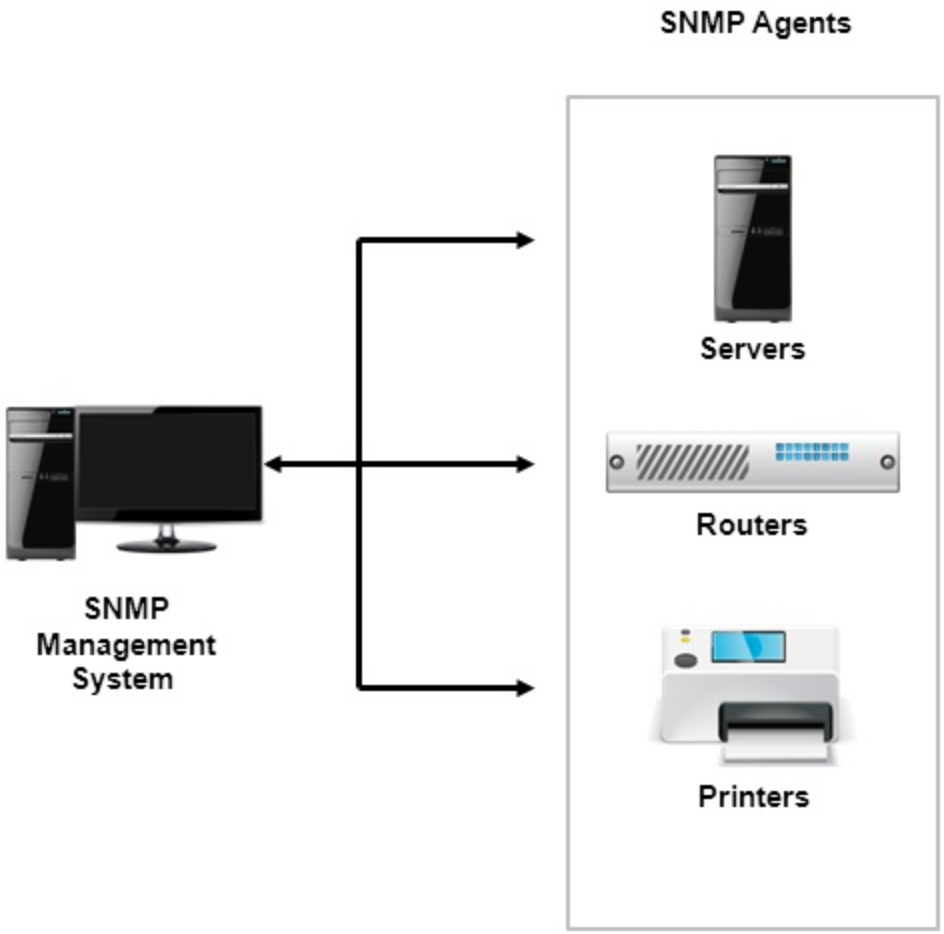


Figure: SNMP collects information from network devices for diagnostic purposes.

SSH

Secure Shell (SSH) is a protocol that enables a user or application to log on to another computer over a network, execute commands, and manage files. It provides strong authentication methods and secure communications over insecure channels. It is a more secure version of remote connection programs that transmit passwords unencrypted, such as Telnet. With the SSH

```
slogin
```

command, the entire login session, including the password, is encrypted and protected against attack.

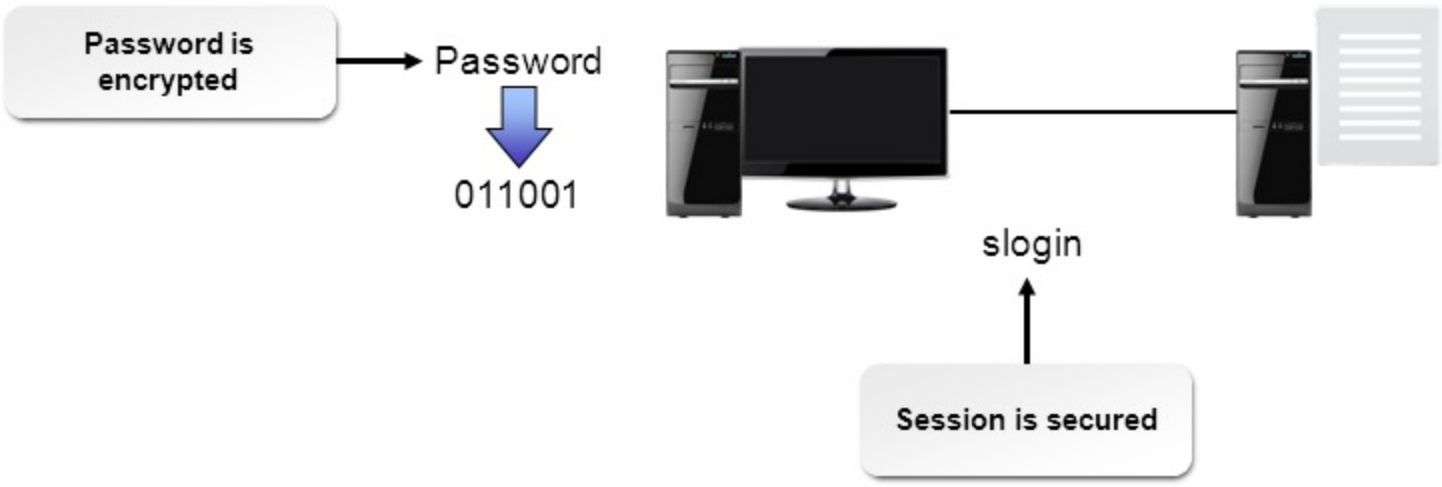


Figure: SSH.

SSH1 and SSH2

There are two versions of Secure Shell available: SSH1 and SSH2. They are two different protocols and encrypt different parts of a data packet. To authenticate systems, SSH1 employs user keys, to identify users; host keys, to identify systems; session keys, to encrypt communication in a single session; and server keys, which are temporary keys that protect the session key. SSH2 is more secure; it does not use server keys. Because they are different protocol implementations, SSH1 and SSH2 are not compatible with each other.

SFTP

Secure FTP (SFTP) is a more secure replacement for FTP that uses the SSH protocol to manage, transfer, and access files over a secure connection.

Note: Note that the acronym SFTP is used both for Secure File Transfer Protocol as well as for the now obsolete Simple File Transfer Protocol.

SMB

The *Server Message Block (SMB)* is a protocol that works on the Application layer and helps share resources such as files, printers, and serial ports among computers. In a TCP/IP network, NetBIOS clients, such as Windows systems, use NetBIOS over TCP/IP to connect to servers, and then issue SMB commands to complete tasks such as accessing shared files and printers.

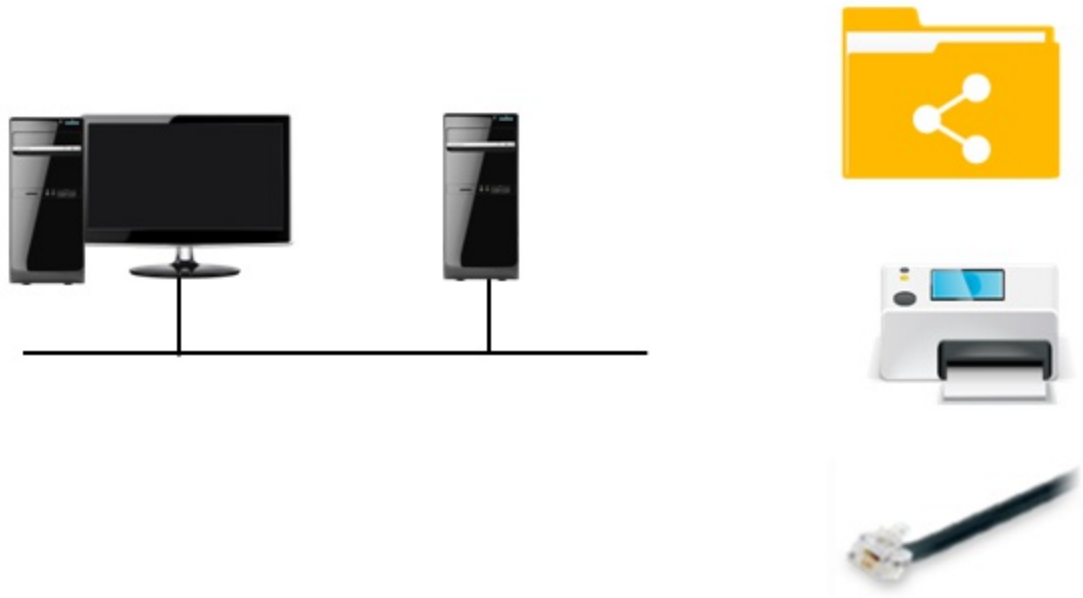


Figure: Resource sharing using SMB.

Topic E: Networking Tools

Now that you have covered all the different network types, configurations, and connection methods, you are ready to take a closer look at tools used to properly install, configure, and maintain all parts of a network.

Working with networks can be challenging depending on the size, location, and environment. In order to properly and safely work with networking components, you must understand how networking tools are used and how they can be used to fix common issues found in networks.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 2.10: Given a scenario, use appropriate networking tools.

Cable Testers

A *cable tester,* also called a *media tester,* is an electrical instrument that verifies if a signal is present on a network cable. A simple cable tester will determine whether a cable has an end-to-end connection and can detect shorts or opens, but it cannot certify the cable for transmission quality.

Figure: A cable tester.

Crimpers

A *wire crimper* is a tool that attaches media connectors to the ends of cables. You can use it if you need to make your own network cables or trim the end of a cable. There are different crimpers for different types of connectors, so select the one that is appropriate for the type of network media you are working with. A *wire stripper* is often part of a wire crimper, allowing the user to strip wires of their protective coating, and then use the crimping tool to attach a media connector.

Figure: A wire crimper.

Multimeter

A *multimeter* is an electronic instrument used to measure voltage, current, and resistance. It usually has two probes with leads, one red and one black, that are plugged into two sockets on the meter. To switch between measuring volts, ohms, and amps, the leads can be moved to different sockets, or there may be a selector switch. Digital meters have a screen that displays the numeric value of what you are measuring. Analog meters have a thin needle that swings in an arc and indicates the value of what you are measuring. Many meters also have specific settings for testing circuit continuity, diodes, or battery charges. Multimeters are sometimes called volt-ohm meters.

Note: Use a digital multimeter whenever possible. It is much more difficult to read and interpret an analog multimeter accurately.

Figure: Multimeters.

Toner Probe

A digital toner and toner probe traces and locates voice, audio, and video cabling on a network. In addition to confirming the cable location, a toner and probe can verify continuity and detect faults.

Figure: A toner probe.

Loopback Plug

A *loopback plug* is any tool that causes the device to transmit a signal back to itself. It is typically used for diagnosing transmission problems that redirects electrical signals back to the transmitting system. It typically plugs into a port and crosses over the transmit line to the receive line. Many times technicians will construct their own device based on their specific needs, but it can be used to test Ethernet network interface cards (NICs).

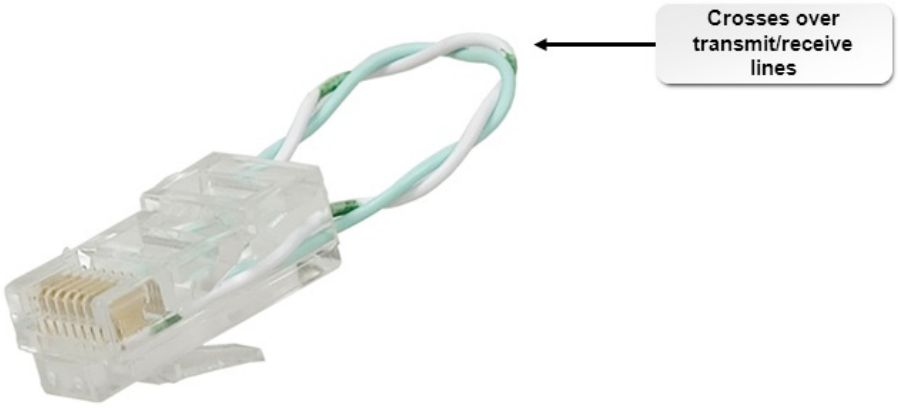


Figure: A loopback plug.

Punch Down Tool

A *punch down tool* is used in a wiring closet to connect cable wires directly to a patch panel. The tool strips the insulation from the end of the wire and embeds the wire into the connection at the back of the panel. The punch down tool makes connecting wires to a patch panel easier than it would be to connect them by hand. Without the punch down tool, you would have to strip the wire manually and connect it by twisting it or tightening it around a connection pole or screw.

Note: The technical name for a punch down tool is an Insulation Displacement Connector (IDC).

Figure: A punch down tool.

Networking Utilities

Microsoft includes a variety of tools in its Windows operating systems that you can use to troubleshoot TCP/IP.

Tool	*Use To*
`ipconfig`	Verify the configuration of TCP/IP and to release or renew DHCP IP address leases. (Other operating systems use different commands rather than `ipconfig`. For example, Linux uses `ifconfig`.)
`ping`	Test TCP/IP communications. With the `-t` switch, you can ping the indicated host until the request gets interrupted; with the `-l [number]` switch, you can send a ping of a specified buffer size.
`nslookup`	Verify that the computer can connect to a DNS server and successfully find an IP address for a given computer name.
`tracert`	Determine and test all points along the route the computer uses to send a packet to a destination. If tracert is unsuccessful, you can use the results generated to determine at what point communications are failing.
`netstat`	Show the status of each active network connection; `netstat` will display statistics for both TCP and UDP, including protocol, local address, foreign address, and the TCP connection state. Because UDP is connectionless, no connection information will be shown for UDP packets.
`net`	Manage Microsoft network resources from a command line. With the `use` option, you can connect or disconnect the computer from a shared resource. You can also retrieve information about current network connections. To see all of the available commands in this suite, type `net /?` at a command line.
Device	Depending on whether you are using a wired or wireless network connection, the

connection status	connection status might be called something like *Local Area Connection* or *Wireless Network Connection.* Verify that the device is connected to the network and able to send and receive data.
Network troubleshooters	Walk you through the resolutions to various common network problems. There are several network-related troubleshooters in the **Help and Support Center** that can help.

Ipconfig Options

The

`ipconfig`

command provides several options that are helpful for network maintenance and troubleshooting.

Command	*Enables You To*
`ipconfig /all`	View the computer's host name, DNS domain name, network card driver, IP address, subnet mask, default gateway, DNS server(s), and WINS server(s). In addition, you can use this display to determine whether the computer was configured through DHCP or APIPA. If the computer obtained its addressing through DHCP, you also see the IP address of the DHCP server.
`ipconfig /release`	Release the IP addressing information assigned to the computer by the DHCP server or APIPA.
`ipconfig /renew`	Lease IP addressing information from a DHCP server or APIPA. If the computer already has a good IP addressed leased, it will not renew unless you release the address first.
`ipconfig /flushdns`	Clear DNS information on the client so that client updates with new configuration information more quickly.
`ipconfig /registerdns`	Register the client with its DNS server.

ACTIVITY 6-4: Identifying Networking Tools

Scenario

In this activity, you will identify networking tools.

1. **You need to determine if a cable is carrying a signal. Which networking tools might help you?**

   __ Crimpers
   _x_ Cable testers
   _x_ Multimeters
   __ Toner probe
   __ Punch down tool

2. **You need to connect cable wires to a patch panel. Which networking tool might help you?**

   __ Crimpers
   __ Loopback plug
   _x_ Punch down tool
   __ Toner probe

3. Open a command prompt.
   a. Select **Start.**
   b. In the **Search programs and files** text box, enter ***cmd***
   c. Select **cmd.**
4. Display and examine the TCP/IP configuration information for your computer.
   a. Enter ***ipconfig /all***
   b. Scroll through the results of the command as your instructor describes the information that is displayed.
5. Verify network connectivity with the **APLUS-DC** server.
   a. Enter ***ping 192.168.1.10***
   b. Examine the results. Were you able to reach the target computer?
6. Examine the status of network connections on your computer.
   a. Enter ***netstat***
   b. Examine the results as your instructor describes them.
7. View help for the `net` command.
   a. Enter ***net /?***
   b. Enter ***net help***
   c. Examine the results as your instructor describes them.
   d. Select at least one of the `net help` commands (such as `net help view`) and display detailed help information. Share your findings with the rest of the class.
8. Close the command prompt.

Topic F: Install and Configure SOHO Networks

In the last lesson, you covered basic networking concepts, the Transmission Control Protocol/Internet Protocol (TCP/IP) addressing scheme, and how networks are connected. In this topic, you will use that knowledge to install and configure a SOHO network.

SOHO networks are much like the larger corporate networks, just on a much smaller scale. No matter what the size or location of the network, you are still responsible for understanding how it is structured and configured. A+ technicians must understand the needs and complexities of SOHO wired and wireless networks.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 2.5: Compare and contrast wireless networking standards and encryption types.
- Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.

What is a SOHO Network?

A *SOHO network* is a network that provides connectivity and resource sharing for a small office or home office. Generally limited to fewer than 20 computers or nodes, a SOHO network often facilitates sharing of files and printers, as well as services such as email, faxing, and so forth. A SOHO network can contain a combination of wired and wireless computer connections, and all of the computing devices in a SOHO network usually share the same physical location.

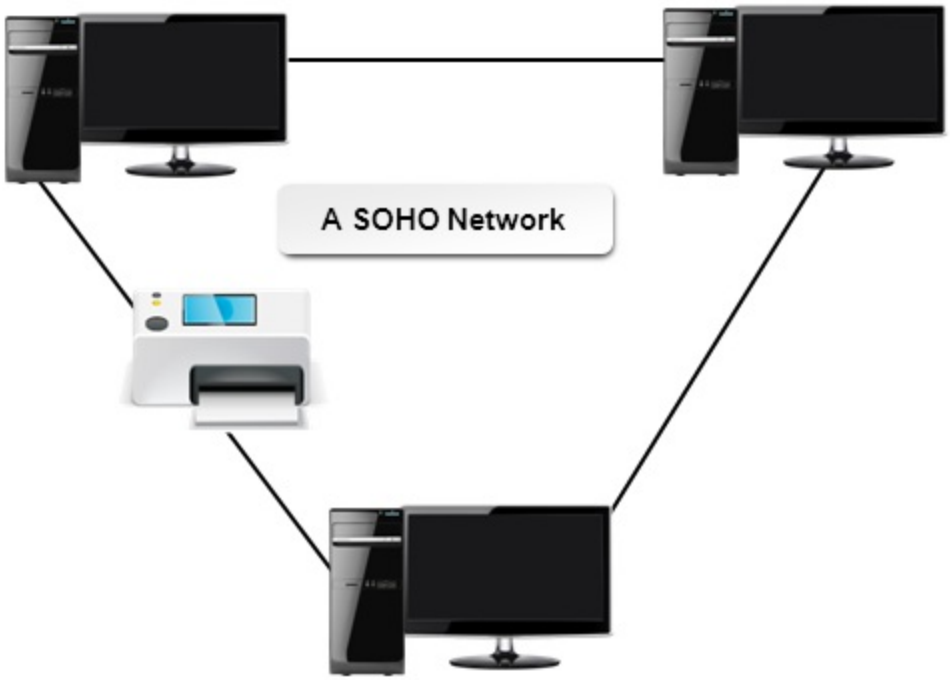


Figure: A SOHO Network.

How Small is Small?

SOHO networks can range in size, and there is no real consensus as to the maximum number of nodes that can be in a SOHO network. Some sources cite the maximum as 10 nodes, while others say that four or five nodes is the maximum.

Firewalls and SOHO Networks

A firewall is a software program or hardware device that protects networks from unauthorized access by blocking unsolicited traffic. Firewalls allow incoming or outgoing traffic that has specifically been permitted by configuring settings. Firewalls use complex filtering algorithms that analyze incoming network data based on destination and source addresses, port numbers, and data type. In many cases a firewall will be the first stop in defending unauthorized access attempts in a SOHO network. Because of the small network size a SOHO the firewall installed must provide the right level of security for the size of the office and the number of connected computing devices.

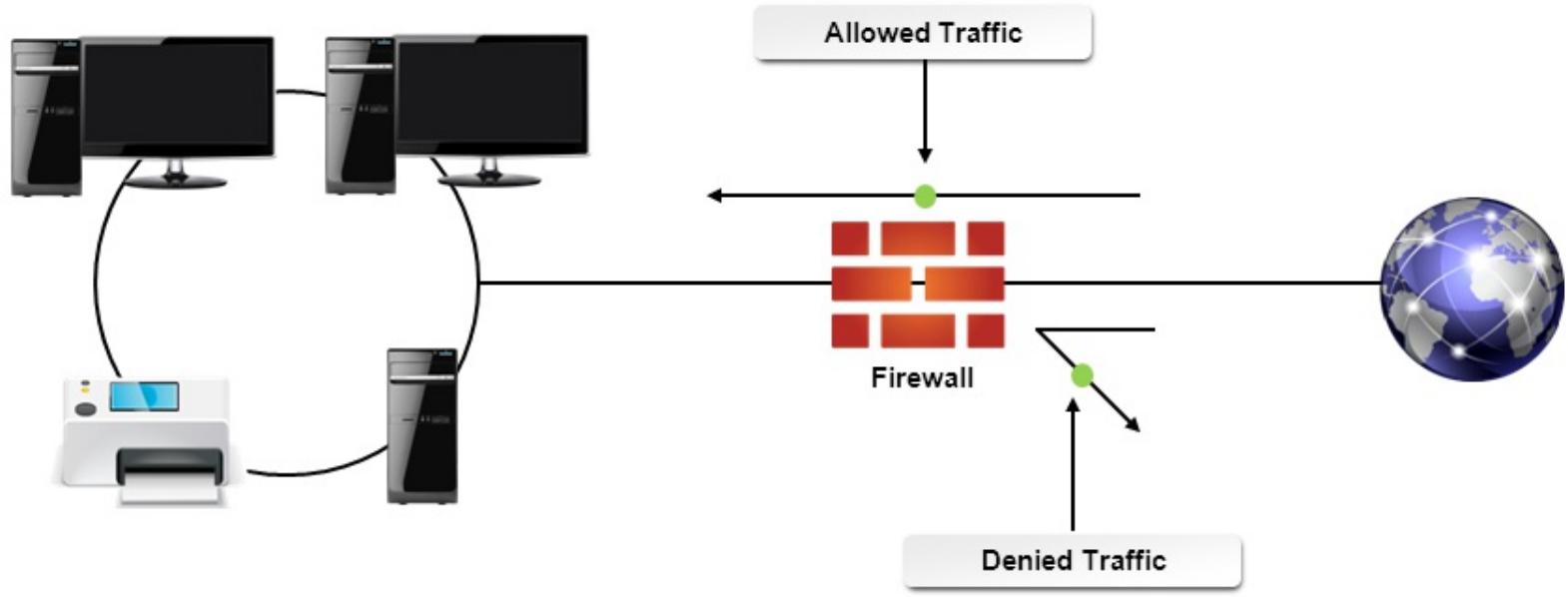


Figure: A firewall in a SOHO network.

Software Firewalls

In some cases a software firewall can be useful for SOHOs. The firewall provides many features that can be configured to suit various computing needs. Some features include:

- Enabling or disabling port security on certain ports.
- Inbound and outbound filtering. The user can set up rules or exceptions in the firewall settings to limit access to the web.
- Reporting and logging activity.
- Malware and spyware protection.
- Pop-up blocking.

- Port assigning, forwarding, and triggering.

Hardware Firewalls

A hardware firewall is a hardware device, either stand-alone or built into most routers, that protects computers on a private network from unauthorized traffic. They are placed between the private network and the public network to manage inbound and outbound traffic and network access.

DMZs

A *demilitarized zone (DMZ)* is a small section of a private network that is located between two firewalls and made available for public access. A DMZ enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole. The external firewall enables public clients to access the service whereas the internal firewall prevents them from connecting to protected internal hosts.

In small offices, DMZs are commonly used to protect any client-facing webservers. This security method prevents any hackers from seeing the private internal IP scheme.

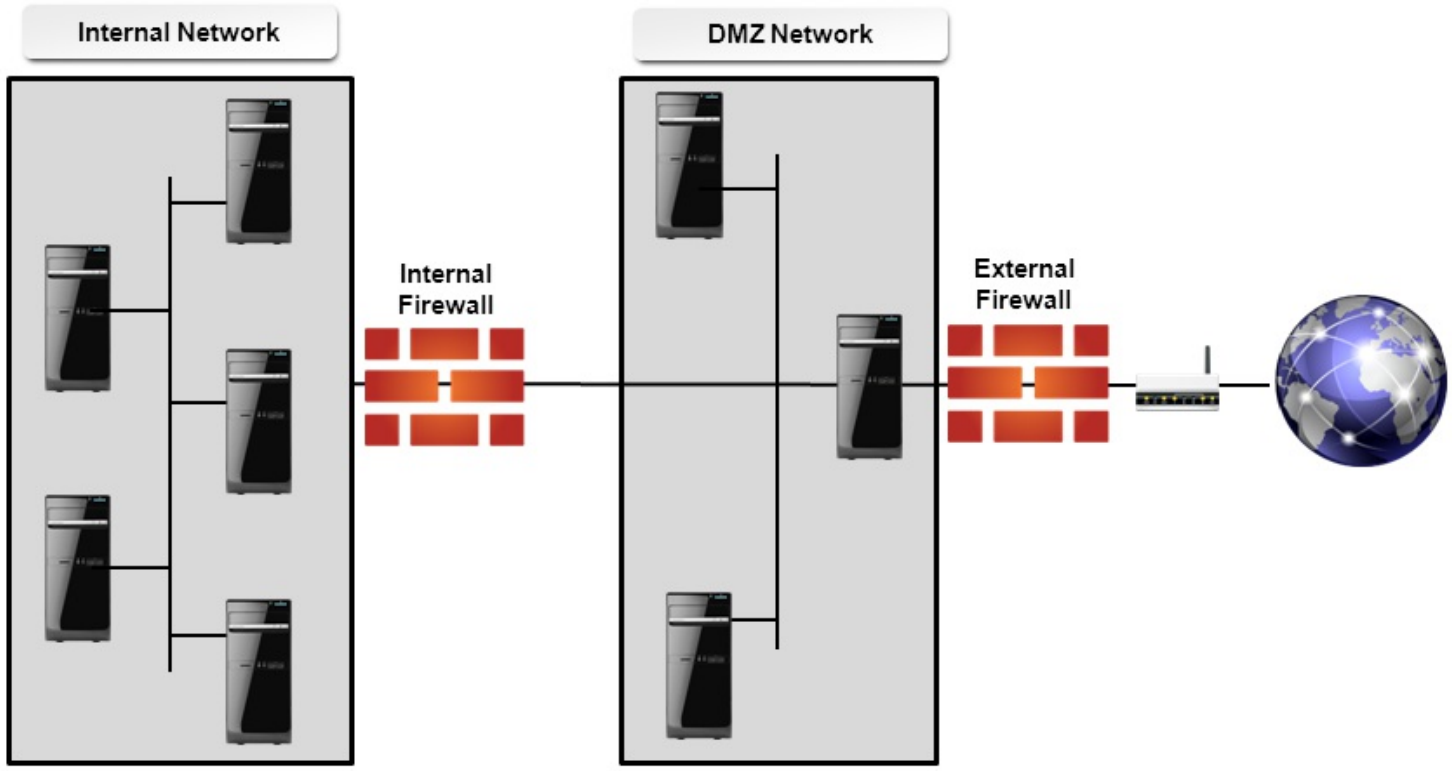


Figure: A section of a private network available for public access.

Other Names for DMZs

DMZs might also be referred to as perimeter networks or screened subnets.

NAT Implementations

Network address translation (NAT) can be implemented as software on a variety of systems or as hardware in a dedicated device such as a router. Internet Connection Sharing (ICS) in Windows systems includes a simple software-based NAT implementation, but requires a separate device, such as a modem, to provide actual Internet connectivity. Hardware-based NAT devices, such as cable modems and DSL routers, often have extended functionality and can double as Internet access devices.

Note: A vast internal network can be configured with a single public address, which makes NAT both secure and cost-efficient.

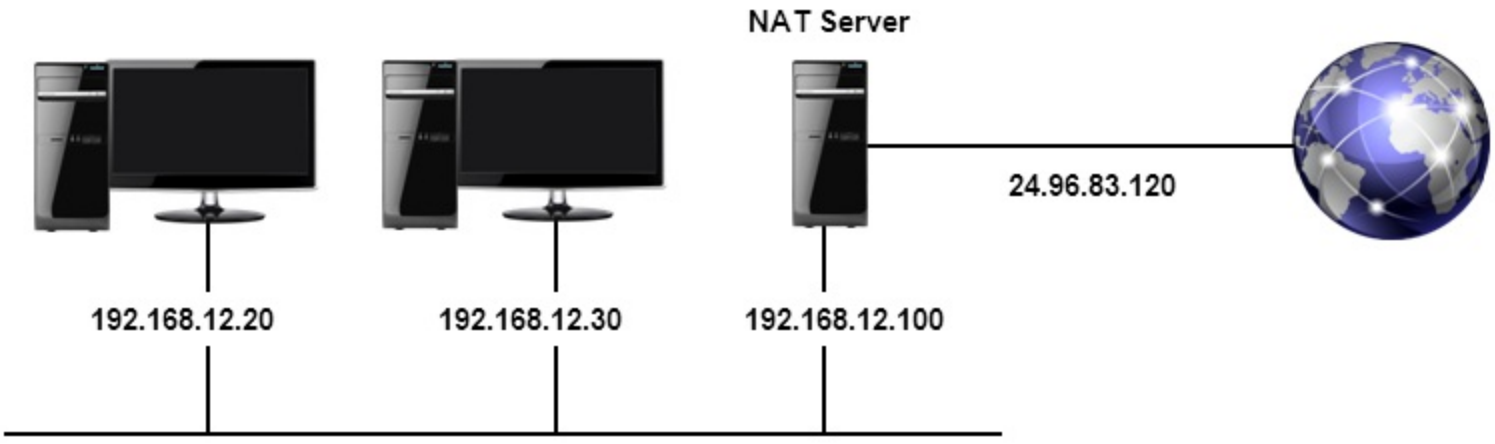


Figure: NAT Implementation.

Static vs. Dynamic NAT

In static NAT, each internal address is mapped to a single specific public address. In dynamic NAT, there is not a one-to-one ratio of internal to external addresses; any number of internal addresses can share a pool of external addresses.

WPS

Wi-Fi-Protected Setup (WPS) is a newer standard that was released in 2007 by the Wi-Fi Alliance to enable an easy yet secure setup of small home networks. The goal of the standard was to ease the setup and complicated configuration settings of wireless routers designed for use in SOHO networks. WPS is a service that comes installed on some routers to support quick secure setups for routers; however, recently the standard has been tainted. The standard has been cracked by brute force attacks and has been reported to be less secure. It is important to fully understand the technology installed on network devices before you connect and install them within your network. In most cases routers come with WPS enabled by default, so you may need to turn it off once the router is connected.

Basic QoS

The amount of data being transmitted over networks is rising every day. Also, the type of data being transferred is changing. Traditional applications such as file transfer protocol (FTP) and Telnet are now outnumbered by real-time multimedia applications such as IP telephony, multimedia applications, and videoconferencing. FTP and Telnet are very sensitive to packet loss but are tolerant to delays in data delivery. The reverse is applicable to multimedia applications; they can compensate for some amount of packet loss, but are very sensitive toward delays in data delivery. Therefore, an optimum usage of bandwidth becomes very critical while dealing with multimedia applications. Low bandwidth may result in a bad quality transmission of real-time applications, leading to dropouts or hangs. In small offices, this issue can be a major problem due to the small network and need to access the Internet. To avoid this, certain parameters were developed to prioritize bandwidth allocation for real-time applications on networks such as the Internet and guarantee a specific QoS.

Quality of Service (QoS) is a set of parameters that controls the quality provided to different types of network traffic. QoS parameters include the maximum amount of delay, signal loss and noise that can be accommodated for a particular type of network traffic; bandwidth priority; and CPU usage for a specific stream of data. These parameters are agreed upon by the transmitter and the receiver, the transmitter being the ISP and the receiver being the subscriber. Both the transmitter and receiver enter into an agreement known as the *Service Level Agreement (SLA).* In addition to defining QoS parameters, the SLA describes remedial measures or penalties to be incurred by an ISP in the event that the ISP fails to provide the QoS promised in the SLA.

Relevance for SOHO Networks

In SOHO networks, network performance degradation can occur when several users are running multiple applications or processes (such as downloads) that consume a lot of network bandwidth. Often, the effects of this are markedly slow Internet connections or connectivity issues with Voice over IP (VoIP) phones. By implementing basic QoS to prioritize services such as VoIP over file downloads and Internet surfing, you can ensure that the services that you decide to prioritize are getting the bandwidth they need.

802.11 Wireless Standards

The *802.11* standard is a family of specifications developed by the IEEE for wireless LAN technology.

802.11 Standard	***Description***
802.11a	*802.11a* is an approved specification for a fast, secure, but relatively expensive wireless protocol. 802.11a supports speeds up to 54 Mbps in the 5 GHz frequency band. Unfortunately, that speed has a limited range of only 60 feet, which, depending on how you arrange your access points, could severely limit user mobility.
802.11b	*802.11b* (also called *Wi-Fi,* short for "wireless fidelity") is probably the most common and certainly the least expensive wireless network protocol. 802.11b provides for an 11 Mbps transfer rate in the 2.4 GHz frequency. Some vendors have increased the rate on their devices. 802.11b has a range up to 1,000 feet in an open area, and a range of 200 to 400 feet in an enclosed space (where walls might hamper the signal). It is not compatible with 802.11a. This standard supports up to 14 channels, but the available channels depend on local regulations. For instance, in areas where the FCC governs, the available channels are channel 1 through channel 11.
802.11e	*802.11e* is a wireless standard for home and business implementations. It adds Quality of Service (QoS) features and multimedia support to 802.11a and 802.11b, and is compatible with those standards.
802.11g	*802.11g* is a specification for wireless data throughput at the rate of up to 54 Mbps in the 2.4 GHz band. It is compatible with 802.11b, and is replacing it due to its faster speed.
802.11n	*802.11n* is a recent specification for wireless data throughput. Even before approval, many "Draft N" or "Pre-N" products were already being produced and sold, compliant with the specification. The specification increased speeds dramatically with data throughput up to 600 Mbps in the 2.4 GHz or 5 GHz ranges.

Note: Home-based Wi-Fi networks are often susceptible to interference from microwave ovens, which also operate in the 2.4 GHz frequency range.

WAPs

A *Wireless Access Point (WAP)* is a device that provides connection between wireless devices and enables wireless networks to connect to wired networks. A WAP is sometimes called just an AP or a WLAN-AP. WAPs have a network interface to connect to the wired network and a radio antenna or infrared receiver to receive the wireless signals. Many include security features that enable you to specify which wireless devices can make connections to the wired network.

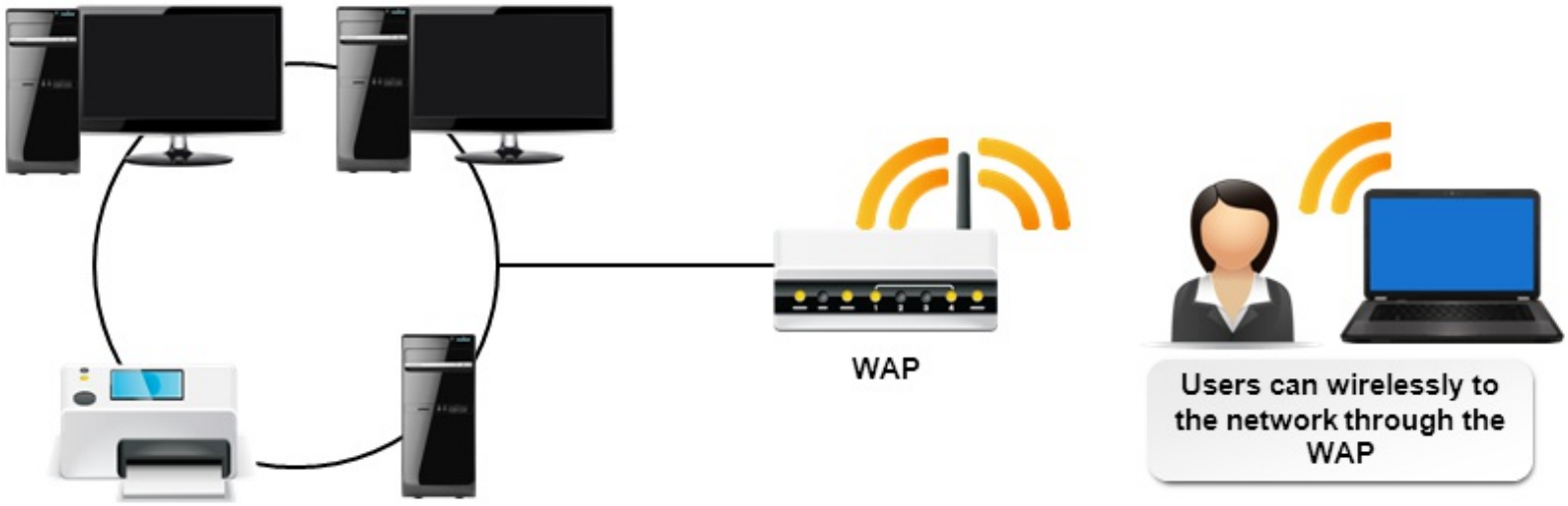


Figure: A Wireless Access Point.

SSID

The *Service Set Identifier (SSID)* is a 32-bit alphanumeric string that identifies a WAP and all devices that connect to it. Since a wireless client device must provide the SSID in order to connect to the WAP, the SSID functions as a sort of password for the wireless network. However, because the WAP typically broadcasts the SSID in plain text, it does not provide any security. It is more realistic to think of the SSID as a network name that is applied to the grouping of the WAP and the devices currently connected to it. The administrator can accept a device's default SSID or specify an SSID manually to more clearly identify the device.

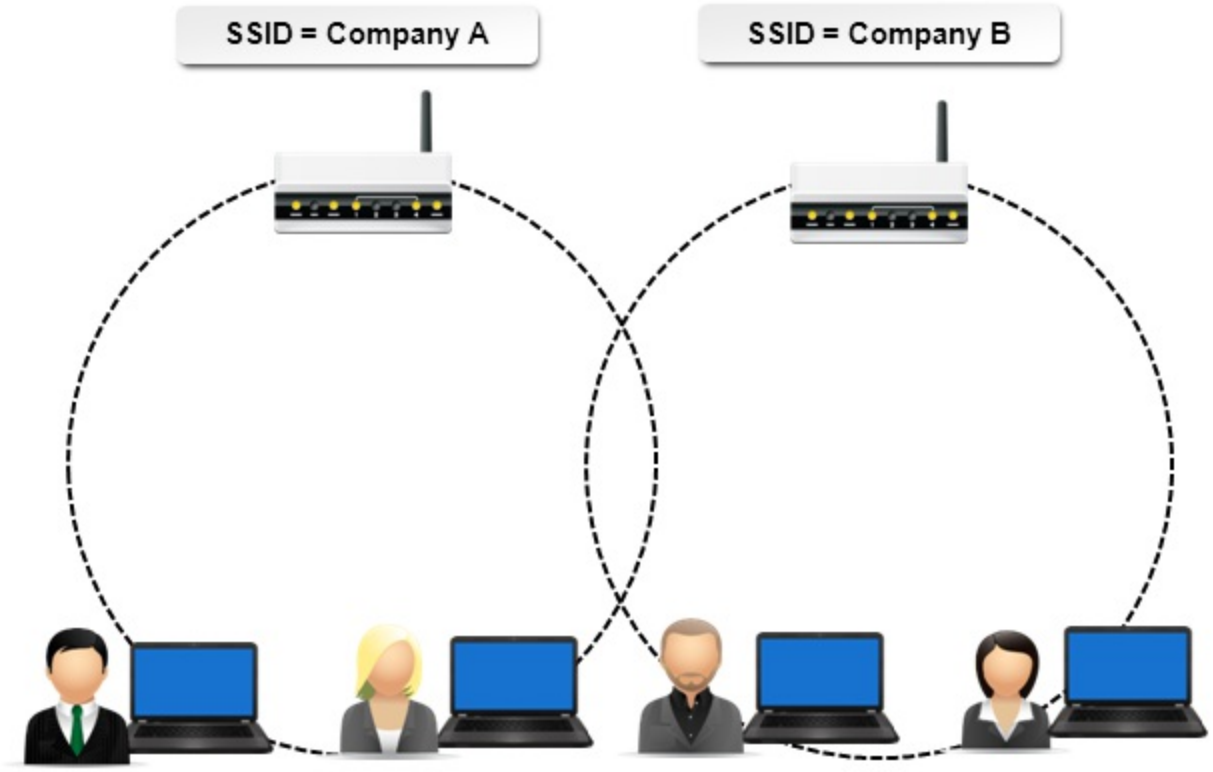


Figure: SSID.

What is Encryption?

Encryption is the process of converting data into a form that is not easily recognized or understood by anyone who is not authorized to access the data. Only authorized parties with the necessary decryption information can decode and read the data. Encryption can be one-way, which means the encryption is designed to hide only the cleartext and is never decrypted, or it can be two-way, in which the encryption can be decrypted back to cleartext and read.

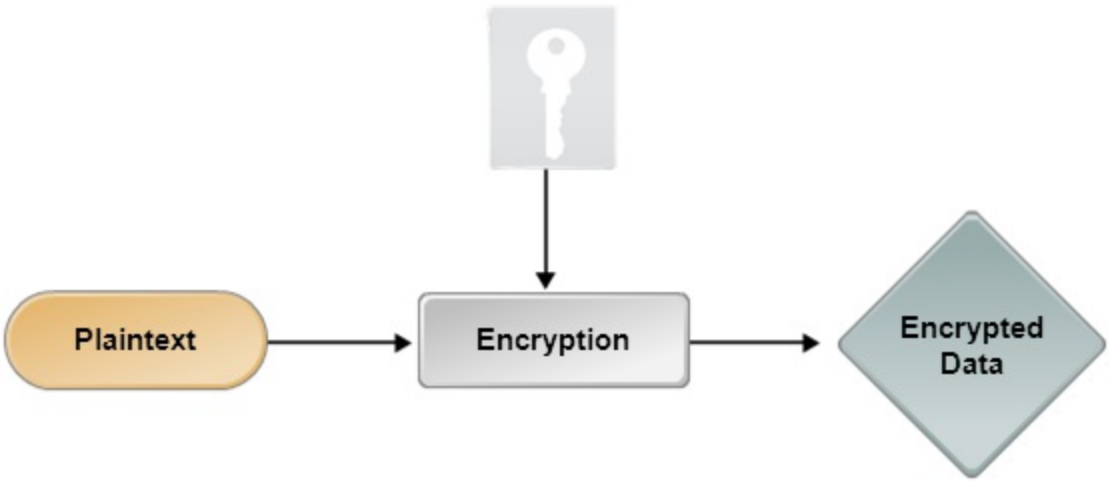


Figure: Encryption.

Wireless Encryption Types

The use of wireless computing devices is rapidly increasing every day. This also increases the risk of wireless security attacks on devices to gain access to secure data and resources. *Wireless encryption* conceals and protects data during transmission so that if the data were accessed during transmission it cannot be read. There are a number of encryption types available to provide encryption over wireless data transmissions.

Wireless Encryption Type	***Description***
WEP	*Wired Equivalent Privacy (WEP)* provides 64-bit, 128-bit, and 256-bit encryption for wireless communication that uses the 802.11a and 802.11b protocols. While WEP might sound like a good solution at first, it ironically is not as secure as it should be. The problem stems from the way WEP produces the keys that are used to encrypt data. Because of a flaw in the method, attackers could easily generate their own keys by using a wireless network capture tool to capture and analyze network data and crack WEP in a short period of time.
WPA	*Wi-Fi Protected Access (WPA)* is a security protocol that was introduced to address some of the shortcomings in the WEP protocol during the pending development of the 802.11i IEEE standard. It uses strong authentication and data encryption mechanisms.
WPA2 or 802.11i	*802.11i* is a complete wireless standard that adds strong encryption and authentication security to 802.11 and relies on 802.1x as the authentication mechanism. 802.11i is sometimes referred to as WPA2. • WPA provides improved data encryption through the *Temporal Key Integrity Protocol (TKIP),* which is a security protocol created by the IEEE 802.11i task group to replace WEP. It is combined with the existing WEP encryption to provide a 128-bit encryption key that fixes the key length issues of WEP. • In addition to TKIP, WPA2 adds *Advanced Encryption Standard (AES)* cipher-based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption for even greater security and to replace TKIP. It provides a 128-bit encryption key. • Both standards have been extended to include several types of user authentication through EAP, which is considered poor in WEP. WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively easy to figure out, steal, and use (that is, sniff and spoof). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Router Settings and Configurations

Most routers available today can be configured for wired and wireless networks. Depending on the router installation, there are a number of settings that can be configured to ensure connectivity, security, and access.

Setting	*Description*
Basics	Basic settings apply to both wired and wireless routers and can include the ability to: • Secure your router or access point administration interface. • Change default administrator passwords (and user names). • Disable remote administration. • Secure/disable the reset switch/function. • Change the default SNMP parameter. • Regularly upgrade the Wi-Fi router firmware to ensure you have the latest security patches and critical fixes.
SSID	When installing a wireless router, change the default Service Set Identifier (SSID) and verify that you are not broadcasting out to the network.
MAC filtering	Apply MAC address filtering to both wired and wireless routers. By configuring a wireless access point (WAP) to filter MAC addresses, you can control which wireless clients may join your network.
Channels	Change the default channel on wireless routers. By changing the router channel, you can optimize data transmission and reduce interference with other routers in close proximity. If your router is dual channel, then you can easily change from the default channel to the other channel available. To help determine what channel is not being used there are utilities available that can scan the local area and display used channels. This can be very helpful in choosing a different less used channel for your router.
DHCP	Depending on the needs of your network, turn on DHCP on both wired and wireless routers to automatically connect and assign an IP address, or turn it off and enter a static IP address.

Port Forwarding and Triggering

If your router has NAT, then you can also configure port forwarding, which forwards a network port from one network node to another, and port triggering, which automates port forwarding by specifying ports (triggering ports) to automatically and dynamically forward inbound traffic to.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Configure SOHO Networks**

Summary

In this lesson, you identified many different network technologies. Networking is at the heart of any type of business. Without it, a business simply cannot function in today's world. It is your job to ensure that the networks behind the business are running properly and managed correctly.

What do you think are the most important network concepts covered in this lesson?

Do you have any experience working with any of these technologies?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 7: Supporting Laptops

Lesson Time: 1 hour

In the previous lessons, the focus has been on installing system components and establishing network connectivity. In this lesson, the focus will be on laptop components and how they differ from the standard system components. As an A+ technician, you will also require a robust knowledge of portable computing principles. In this lesson, you will install and configure various system components and explore the components that make up the laptop.

Laptops are everywhere today. Because of their portability and powerful computing capabilities they are prominent in most workplaces. So, as a certified A+ technician, you will be expected to configure, maintain, and troubleshoot laptop computing devices. With the proper information and the right skills, you will be ready to support these devices as efficiently as you support their desktop counterparts.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Topic A:
  - Objectives 1.3. 3.1, 3.2, 3.3

- Topic B:
  - Objective 3.1

Topic A: Laptop Hardware and Components

You have examined the components of desktop machines in the previous lessons. Similarly, laptops have many of the same components that are configured to fit into a portable format. In this topic, you will examine the hardware components of a laptop.

As a certified A+ technician, you already know a lot about the components of desktop systems. However, you will also be expected to support laptops, and the components are not always the same as their desktop counterparts. Having a solid understanding of laptop hardware components is essential for you to be able to implement and support them properly. The information in this topic should give you the foundation you need to understand the components in the various types of laptops you might be called upon to support.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 1.3: Compare and contrast RAM types and features.
- Objective 3.1: Install and configure laptop hardware and components.
- Objective 3.2: Compare and contrast the components within the display of a laptop.
- Objective 3.3: Compare and contrast laptop features.

Laptops

A *laptop* is a complete computer system that is small, compact, lightweight, and portable. All laptops have specialized hardware designed especially for use in a smaller portable system, use standard operating systems, can run on battery or AC power, and can connect to other devices. Laptops and their components can vary by the following factors:

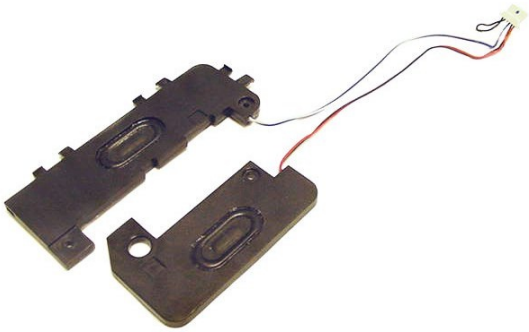
- Size of the device. Smaller models are referred to as notebooks or sub-notebooks and typically have fewer features.
- Display size, quality, and technology.
- Keyboard size, number of keys, and additional options.
- Pointing device used.
- Power supply type.
- Battery type used.
- Length of battery support time.
- How long it takes to recharge the battery.
- Power cord connection and power source options.
- Docking solutions.
- Connections for external peripherals.
- The power button can be located inside or outside of the closed case. It is more often located inside so that it is not accidentally turned on when it is in the user's briefcase or being transported in some other bag.
- Bays or connections for additional drives such as optical drives.

Figure: A laptop.

Laptop Hardware Components

A laptop has many different hardware components that each have unique characteristics and features.

Component	*Description*
Keyboard	The keyboard is an integrated component on a laptop. Not all laptop keyboards can be replaced, so you should check the manufacturers documentation to verify that it can be repaired or replaced.
Touchpad	A touchpad is a small, touch-sensitive pad where you run your finger across the surface to send electronic signals to the computer to control the pointer on the screen. Touchpads can have buttons like a mouse or trackball, or the touchpad can be configured to detect finger taps on its surface and process those signals like a mouse button.
Trackpoint	A *trackpoint,* or pointing stick, is most commonly found on laptops. Located in the center of the keyboard, the trackpoint is a small joystick-like button that responds to user force in all directions in order to move the mouse pointer on screen.
	The *plastics* are the hard surfaces that cover the internal components of the laptop. They are typically secured together using small screws or pressure tabs.

Plastics	
Speaker	The speakers are located in a number locations depending on the style and manufacturer of the laptop. Newer model laptop speakers are just as powerful as the desktop versions. 
Battery	The battery designed for laptops is rechargeable and can easily be removed or replaced. Most batteries will last between one and six hours per charge while extended life batteries have a wide range of limitations based on the manufacturer and what the user is doing with the laptop. Programs that require more computing power and screen updates such as multimedia applications are likely to deplete the battery faster than working on a simple word processing document. Some laptops offer extra battery packs that can be inserted in place of other removable devices, such as optical drives, allowing users to easily reconfigure their laptops for various travel and working situations. Rechargeable batteries are used in most portable computing devices. They are usually packaged in a battery pack. Before replacing a laptop battery you should verify what the system requirements are. New batteries must be compatible with the system.

DC jack	The direct current (DC) jack on a laptop provides power through the power cord. Most laptop DC jacks are specific to the manufacturer and even the laptop model, so make sure to check the documentation for power requirements and compatible power cords.
Screen	The screen is the visual display of a laptop and is typically hinged at the bottom and swings down to form the cover for the laptop. It latches to the body of the computer to secure it for transport.

Integrated Peripherals

Integrated peripherals include the screen, keyboard, and touchpad devices. Not all peripherals can be replaced. Check with the manufacturer of the laptop for guidelines on what components can be replaced and what components cannot.

Types of Laptop Displays

Traditionally, laptop displays used CCFL with an inverter cable. Newer laptops use LCD or LED displays.

Contrast Ratio

The contrast ratio is a metric of a display system, defined as the ratio of the luminosity of the brightest and the darkest color the system is capable of producing. High contrast ratio is a desired aspect of any display.

Laptop Display Components

Within the display unit of a laptop, there are several specialized components, with a unique function.

Component	*Description*
Inverter	An *inverter* is used to convert DC power to AC power for the display. When an inverter fails, depending on the laptop model, it may be appropriate to simply replace the display rather than replace the inverter. Replacement of the inverter requires an exact match, both electrically and mechanically (connectors, size/shape, and mounting).
Backlight	A *backlight* is the typical form of illumination used in a full-sized LCD display. Backlights differ from frontlights because they illuminate the LCD from the side or back, where frontlights are in front of the LCD. *Frontlights* are used in small displays such as on MP3 players to increase readability in low light conditions.
Wi-Fi antenna	The Wi-Fi antenna is typically placed inside the display section of the laptop. The cables are run along the sides of the display unit and connects to the network card inside the main unit of the laptop. It sends and receives wireless signals and transmissions to the WAP.

Internal Laptop Components

The internal components of a laptop are similar to full size desktop computers except that they are much smaller and more compact to fit inside the case.

Component	*Description*
Motherboard	From a technical viewpoint, a laptop system board is very similar to the system boards found in desktop systems. The main difference is that the components are often compressed to squeeze into a smaller space. Other major differences include reduced power consumption and more common integration of items such as video, sound, wired and wireless network connections, USB/FireWire®, and so on. Laptop system boards often contain power management and throttling options to help in preserving battery life. These features allow for the machine to adjust the power to the processor and other components as necessary. The integration of all the features on the motherboard limits customization options and necessitates replacement of the entire board when one of the integrated features fails. However, you may be able to use an alternative slot or port and add an adapter card or an external device to substitute for the failed integrated component.
CPU	Laptop CPUs are designed to use less power and to generate less heat than desktop CPUs, and often are designed to be used without a CPU fan, which, again, saves on size and weight, as well as reducing power consumption to maximize battery life. CPUs can be surface-mounted devices, soldered directly to the motherboard, or attached via a socket on the motherboard. CPUs that are soldered onto the motherboard are not replaceable. It is best to determine how a laptop CPU is attached before trying to replace it.
Hard drive	Portable computer drives are specially designed to fit in portable computers. Drives can be unique to a manufacturer and sometimes even to the computer model. All laptop computers have an internal hard drive. Hard drives come in two main form factors: 2.5 inch and 3.5 inch. The 3.5 inch HDD tends to be too big for laptops, so in most laptops the hard drives the 2.5-inch HDD. Because of their smaller size, the 2.5 inch platters tend to run at slower speeds than the 3.5 inch desktop HDDs. Some internal hard drives are difficult to remove and require dismantling of the computer. Others have a slide lock to unlock them from the case, so that you can slide the drive out. If it is too difficult to remove the internal drive from the notebook you are working on, then you might consider using alternate hard drive solutions such as USB or FireWire hard drives that can be connected externally.
	Portable devices use memory that was specifically designed for those devices. Since it is not produced in as high quantities as desktop memory, it tends to be more expensive.

Memory	While some laptops use SODIMM modules, which are about half the size of standard desktop DIMMs, or *MicroDIMMs,* many require non-standard proprietary memory that must be ordered from the manufacturer. Other portable computing devices and some notebooks use flash memory modules rather than regular RAM. Be sure to check the documentation for your device so that you purchase the correct type of memory. Before you replace the memory in a laptop, you must verify that it is compatible with the system. Always check the manufacturer's documentation or website to verify the form factor and types of compatible memory.
Optical drive	Optical drives in laptops are similar in function to the full size desktop models except that they are small and more compact. When replacing a drive, the first thing to do is check with the manufacturer to verify that it can be replaced and with what type of drive. You need to make sure that the drive you install in compatible with the laptop.
Wireless card	In some laptops, the wireless card and video card can be upgraded to improve performance. However, replacement is dependent on whether the card is an integrated component of the mobile system board. In this case, you cannot upgrade or replace the card. If the card is independent of the system board, then you should refer to the manufacturer's documentation to verify what components can be replaced and upgraded. Some components may be covered under a system's warranty, so refer to the manufacturer's policies to determine what can be upgraded without breaking the warranty guidelines.

Laptop Memory Package Specifications

The following table lists some of the technical specifications for laptop memory packages.

Memory Package	***Description***
SODIMM	Small Outline Dual Inline Memory Module. Used in some notebook systems and Apple® iMac® systems. Measures about 2 inches by 1 inch and has 144 pins. Capacity ranges from 16 to 256 MB per module.
MicroDIMM	Micro Dual Inline Memory Module. Used in small, sub-compact notebooks. Measures about 1.5 inches long and has 144 pins.

	Capacity ranges from 512 MB to 1 GB.

Laptop Expansion Options

Laptop systems offer many different options to expand system functionality. Slots and ports located on the outside of the case can allow you to add compatible expansion cards to the system. There are a number of different expansion cards available.

Expansion Card	***Description***
PC Cards	Designed by the *Personal Computer Memory Card International Association (PCMCIA)*, these cards were originally referred to as PCMCIA Cards. *PC Cards* are credit-card-sized expansion cards that are used in portable computers rather than the full-sized expansion cards used in desktop systems. PC Card expansion slots provide additional functionality to laptop systems. Cards are 4 mm wide by 85.6 mm long, and have a female 68-pin connector that plugs into a 68-pin male connector inside a slot in the side of the computer. There are currently three types of approved cards: • Type I: 3.3 mm thick, with a 16-bit interface. Typically used for memory devices. • Type II: 5.0/5.5 mm thick, with a 16- or 32-bit interface. Typically use a *dongle* to connect to a full-size connector. • Type III: 10.5 mm thick, with a 16- or 32-bit interface. Hard disk drive cards are Type III.
ExpressCards	*ExpressCards* are mobile expansion cards designed by the PCMCIA to replace traditional PC Cards. The ExpressCard slot on mobile devices provides PCI Express and USB 2.0 connectivity. The two form factors available for the ExpressCard are the ExpressCard/34 (34 mm wide) and ExpressCard/54 (54 mm wide). ExpressCard slots are a bit smaller than the PC Card slots and are usually located on the side of the laptop. ExpressCards can be used to provide many additional functions such as wireless network access, USB ports, and others. The ExpressCard technology has many advantages over the PC Card, including reduced voltage usage, increased bandwidth, and a maximum throughput of 2.0 Gps through PCI Express and 480 Mbps through USB 2.0. Some manufacturers are providing both PC Card slots along with ExpressCard slots to comply with both standards.
	Some portable systems include a PCI Express Mini Card (Mini-PCIe) slot. A *Mini-PCIe* card is an extremely small expansion card, often just a few centimeters in length. Unlike PC Cards, Mini-PCIe cards are internal and are installed by the computer manufacturer. Mini-PCIe cards are most often used to increase communication abilities by providing network adapters or modems and supports various connections and

Mini-PCIe	buses: • USB 2.0. • Diagnostic wiring that provides LED for wireless network connectivity. • System management Bus (SmBus).
SODIMM and Flash memory	Portable devices use memory that was specifically designed for those devices. Since it is not produced in as high quantities as desktop memory, it tends to be more expensive. While some laptops use SODIMM modules, which are about half the size of standard desktop DIMMs, or MicroDIMMs, many require non-standard proprietary memory that must be ordered from the manufacturer. Other portable computing devices and some notebooks use *flash memory* modules rather than regular RAM. Flash memory is a type of non-volatile storage method that provides devices with quick access to data. Be sure to check the documentation for your device so that you purchase the correct type of memory.

Special Function Keys

Laptops are all so different and the features can vary based on the manufacturer. A common feature included in most devices are the special function keys. The specific keys available will depend on the size, shape, and overall design of the laptop but most systems will provide the basic keys. The special keys are typically positioned horizontally along the top length of the keyboard and allow users to launch operating system commands, and manage laptop settings from their keyboard in many ways:

- Switching between single and dual displays.
- Turning the wireless on and off.
- Changing the volume of the speakers.
- Managing the screen brightness.
- Turning the Bluetooth® on and off.
- Configuring the keyboard backlight.

Figure: Special function keys.

Laptop Docking Solutions

One of the most attractive features of laptops is that they are so portable. They can be docked and undocked quickly for transport. Docking solutions provide users with a power source and full size peripherals with a similar feel to a full size desktop computer. There are a few different docking options depending on the specific needs of the user.

Docking Solution	***Description***
Docking station	A *docking station* is used when a laptop computer replaces a desktop computer. This technology is rarely used today and is considered to be legacy hardware. The laptop is connected to the docking station through a docking port located on the back or bottom of the laptop. Docking stations typically extend the capabilities of the laptop by providing additional interfaces for the laptop. In addition, there are often slots for desktop PCI or ISA expansion cards, drive bays for additional mass storage devices, and possibly additional ports and connectors, such as extra USB or wireless connections.
Port replicator	A *port replicator* is a scaled-down version of a docking station that presents the interfaces that the laptop already has. It contains connections for the standard ports, such as power, keyboard, mouse, and display, but it generally does not support additional expansion cards or drive bays, although some port replicators will contain extra USB or wireless connections.
Media/accessory bay	Some portable computing devices offer media/accessory bays to allow a user to expand the functionality of the device. Such bays often accept optical drives, secondary hard drives, or secondary batteries. These bays are typically proprietary and the accessories for the bays must be ordered directly from the device manufacturer. Most laptops today will utilize wireless peripherals and USB attached drives, so USB hubs and media bays are not used as much anymore.

Laptop Locks

Because laptops are so portable, they are easily lost or stolen. Another feature of laptops is the ability to attach a physical laptop lock or a cable lock. A physical cable lock attaches to the laptop using one of the compatible slots. The cable is then secured around a permanent object. The lock is usually accessed using a combination or a key. Depending on the lock, it may attach to the VGA or printer port. The locks come with special screws that secure the lock in place. The Kensington lock is a cable lock that inserts into a specifically designed port on the laptop. After the Kensington cable was released, laptop manufacturers named the special port the Kensington lock port.

Figure: Kensington laptop locks.

Laptop Power Supplies and Batteries

Laptops can use either AC power sources (alternating current from an electrical outlet) or DC power sources (direct current from a battery). While the laptop is in its portable state, it uses batteries. When the device is used as a desktop computer or peripheral, it can use either batteries or AC power.

AC power connectors vary from device to device. It is important that a laptop not be used with a power cord other than the one provided by the manufacturer. When the laptop is not being used as a portable device, it is usually plugged in using the AC power cord that matches the computer. The battery is also recharged through this connection.

Auto-Switching and Fixed Input Power Supplies

Power supplies with voltage selector switches are called fixed-input power supplies. The voltage selector switches generally have two settings—for example, 220 and 110—depending on the manufacturer. If you set the switch to a higher voltage than supplied by the power source, the system will not receive enough power and will not function properly. However, if you set the switch to a lower setting than supplied by the power source—for example, if you set the switch to 110V while connected to a 220V outlet—you run the risk of burning out the power supply, damaging system components, or more seriously, creating a fire or electrocution hazard.

Auto-switching power supplies do not have a manual voltage switch, but detect the voltage level supplied by the outlet and set themselves to the correct voltage automatically. This can be convenient and safe for people who travel to various countries with portable computers.

Laptop Cooling Considerations

Heat can be a considerable problem with laptops due to their compact size and integrated design. The components are all within close proximity and can generate a lot of heat. There are a number of cooling methods and considerations used to keep the devices within a safe heat range for operation:

- Laptop CPUs are engineered to draw less power and thus run cooler than their similarly rated desktop counterparts.
- Fans are used to move the hot air out from the inside of the laptop case.
- Limit the use of the laptop battery as much as possible. The battery itself can be a heat source.
- Laptop cooling pads are accessories that are designed to sit under the laptop to protect a user from getting a burn from a device overheating. The cooler is placed underneath the laptop to move the air away from the device.

ACTIVITY 7-1: Identifying Laptop Components

Scenario

In this activity, you will examine a laptop and identify its components.

1. Examine a laptop and identify the external components such as the keyboard, display, track point or touch pad.
2. What type of screen display does the laptop have?
3. Locate the battery. Is it visible from the outside, or is it an internally mounted battery?
4. What special function keys does the laptop have?
5. Does the laptop have a Kensington cable lock port?
6. What expansion options are available on the laptop?

Topic B: Install and Configure Laptop Hardware Components

In the previous topic, you identified the internal and external components of laptops. Now that you understand how all these components fit together, you are prepared to install and configure them. In this topic, you will install and configure laptop hardware components.

Laptops are extremely popular in the business, personal, and recreational markets. With these devices now so prevalent, having the skills to install, configure, and support the various components is very important. As an A+ technician, you will use the skills and information in this topic to install and configure laptop components.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 3.1: Install and configure laptop hardware and components.

General Laptop Support Guidelines

There are some general guidelines that can be helpful when supporting laptops within the workplace. With the increased use of smaller laptop devices, you should be aware of the issues and best practices applied when working with the hardware components:

- Verify that there are adequate cooling methods installed and used. Overheating is a serious issue when operating laptops.
- Be aware of the device's warranty restrictions and guidelines. You never want to break a warranty by opening the case or replacing an integrated component that may have been fully covered by a warranty.
- Be careful of the wires that pass through the hinges of a laptop. They can be easily damaged when replacing a display, or screen.

LearnTO: For additional information, check out LearnTO **Install RAM in a Laptop** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

LearnTO: For additional information, check out LearnTO **Replace a Laptop Battery** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Power and Dock a Laptop**

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install or Replace a PC Card**

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install an Express Card**

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install and Replace RAM in a Laptop**

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Replace Laptop Components**

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Replace a Laptop Motherboard**

ACTIVITY 7-2: Installing Laptop Components

Scenario

In this activity, you will examine the internal components of a laptop.

1. Following the manufacturer's instructions or your instructor's guidance, remove the outer case from the laptop.
2. Locate the memory module.
3. Locate the hard drive.
4. Locate the fan.
5. Reassemble the laptop.

Summary

In this lesson, you supported laptop computers by identifying the basic components and installing and configuring external and internal hardware components. With these skills you will be ready to provide the right level of support to your clients or organization in the future.

What is your experience with replacing laptop components?

What type of laptop support do you foresee having to provide to clients in the future?

Social: Check your **LogicalCHOICE Course** screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Lesson 8: Supporting Printers

Lesson Time: 1 hour

In previous lessons, you have installed, configured, and managed system hardware for desktops, laptops, and mobile devices, as well as networking components on all three systems. The next logical step is to examine some of the most common external devices in use on personal computer systems: printers. In this lesson, you will support printers.

Despite predictions that computers would bring about a paperless office environment, the need to transfer digital information to paper or back again remains as strong as ever. Therefore, printing and scanning are among the most common tasks for users in almost every home or business environment. As an A+ certified professional, you will often be called upon to set up, configure, and troubleshoot printing environments, so you will need to understand printer technologies as well as to perform common printer support tasks.

This lesson covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Topic A:
  - Objective 4.1

- Topic B:
  - Objectives 4.2, 4.3

Topic A: Printer Technologies

In this lesson, you will support printers. Before you can provide the right level of support, you must fully understand how these systems are used in a production environment. You need to understand how the various printer components work within a printer to provide the desired outputs. In this topic, you will identify printer technologies.

As a professional support technician, you might be supporting the latest cutting-edge technology, or you might be responsible for ensuring that legacy systems continue to function adequately. So, you must be prepared for either situation and be able to provide the right level of support to users and clients. Having a working knowledge of the many printer technologies and components will help you to support users' needs in any technical environment.

This topic covers all or part of the following CompTIA® A+® (2012) certification objectives:

- Exam 220–801: Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process.

Printers

A *printer* is a device that produces text and images from electronic content onto physical media such as paper, photo paper, and labels. A printer is one of the most popular peripheral devices in use in most computing environments. Printers employ a range of technologies; the quality of the print output varies with the printer type and generally in proportion to the printer cost. A printer output of electronic documents is often referred to as "hard copy." Printers can connect to computers using a variety of connection types, with the most popular methods being USB, networked, and wireless.

Figure: Printers.

Microsoft Printing Terminology

Some Microsoft technical content makes a firm distinction between the software components that represent the printer, and the physical printer itself. You may find that Microsoft refers to the software representation of the printer as the "printer object," "logical printer," or simply "printer," and refers to the printer itself as the "print device" or "physical printer." However, Microsoft sometimes also uses the word "printer" as in common usage, to mean the physical print device. Be aware of the context usage of the terms.

MFDs

A *multi-function device (MFD)* is a piece of office equipment that performs the functions of a number of other specialized devices. MFDs typically include the functions of a printer, scanner, fax machine, and copier. However, there are MFDs that do not include fax functions. Although the multi-function device might not equal the performance or feature sets of the dedicated devices it replaces, multi-function devices are very powerful and can perform most tasks adequately and are an economical and popular choice for most home or small-office needs.

Figure: An MFD.

Types of MFDs

MFDs can be broadly classified into three types, based on their size, cost, and functions.

Type of MFD	***Description***

All-in-one (*AIO MFD*)	These MFDs are small in size and include basic features of printing, scanning, and copying that are required for home users. Interestingly, some of them include features such as *PictBridge* and smart card readers that are not available on high-end MFDs. They have limited or no fax features and do not support networking.
SOHO MFD	These MFDs are medium sized and are designed specifically for small and home offices. They can be connected to a network and can perform tasks at a faster pace than AIOs. They usually have enhanced faxing capabilities and some high-end models are loaded with additional time-saving features, such as an automatic document feeder, duplex printing, *duplex scanning*, extra paper trays, and stapling.
Heavy-duty MFD	As the name suggests, these MFDs are large, network-enabled machines that can cater to the documentation needs of an entire office. They may not include a fax. They are built to handle large volumes of printing, scanning, and copying. Additional features such as automatic document feeder, duplex printing and scanning, and enhanced storage space are available by default.

Laser Printers

A *laser printer* is a printer that uses a laser beam to form images and toner to print the images on a printing medium, such as paper or photo paper.

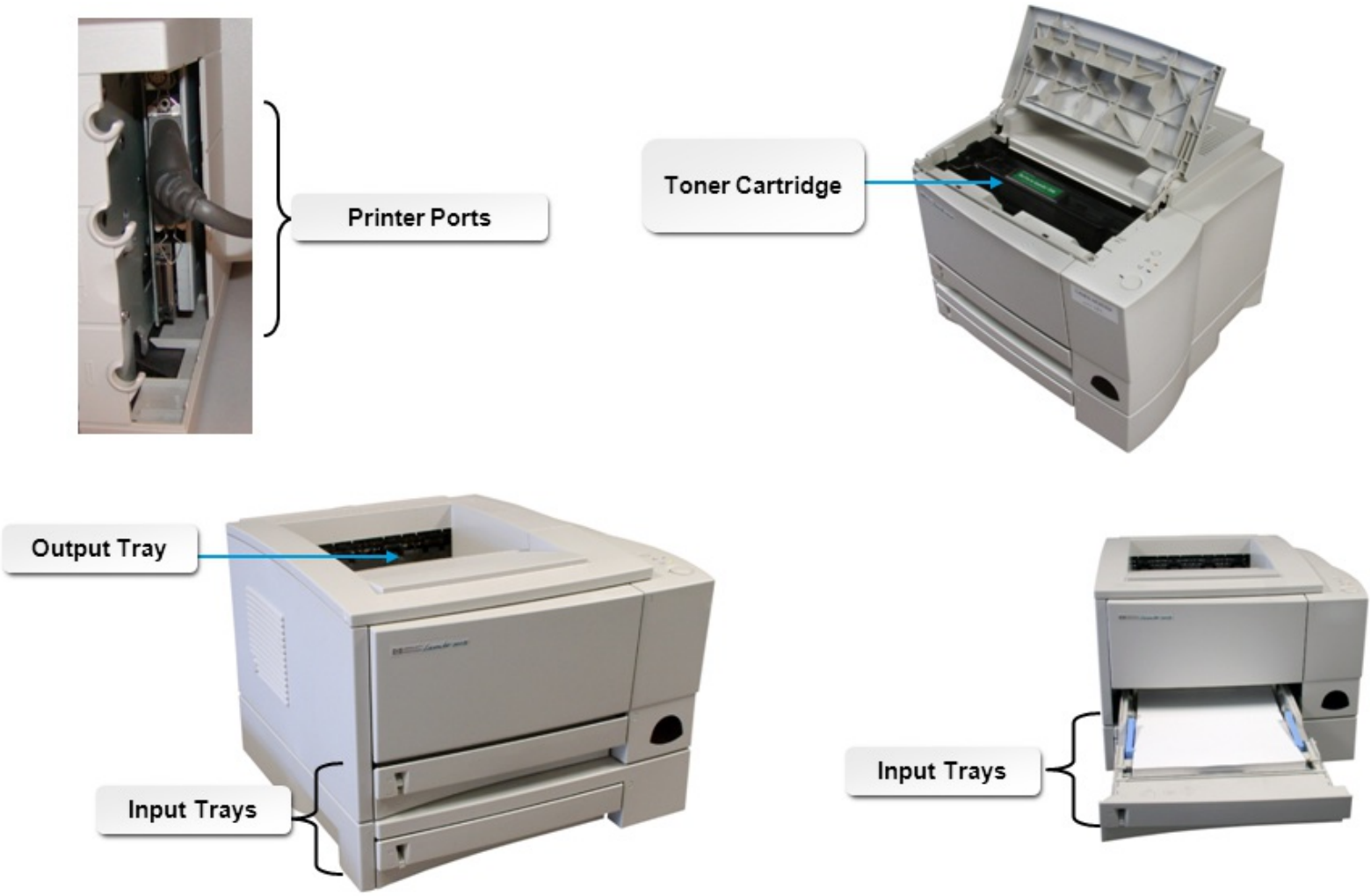


Figure: A laser printer.

Components of Laser Printers

Laser printers include some specialized components not found in other printer types:

- *Toner* cartridge. This is a single, replaceable unit that contains the fine powder used to create images as well as additional components used in image production. Frequently, the EP drum is also incorporated in this cartridge.
- Laser scanning assembly. This is the unit that contains the laser.
- High-voltage power supply. This component converts the supplied current to optimal voltage for specific components and also converts the supplied alternating current (AC) to direct current (DC) for specific internal parts of the printer.

- Paper transport mechanism. This includes the transfer belt and separator pads that move the paper through the laser printer. If the printer is equipped with a duplexing assembly, then the rollers and motors will flip the paper and feed it through to the imaging drum twice.

- *Electrostatic Photographic drum (EP drum)*, or imaging drum. This component carries an electrical charge that attracts the toner. It then transfers the toner to the paper.

- Transfer *corona* assembly. This is a component that contains the corona wires; it is responsible both for charging the paper so that it pulls the toner off the drum and also for charging the drum itself.

- *Fuser assembly*. This unit, also known as the fuser, applies pressure and heat to the paper to adhere the toner particles to the paper.

- Formatter board. This unit exposes and processes all of the data received from the computer and coordinates the steps needed to produce the finished page.

LED Printers

LED printers are similar to laser printers but use the latest printing technology, namely Light Emitting Diodes (LEDs), to replace the laser beam. Some LED printers can print 420 pages per minute.

The Laser Print Process

In the laser printing process, laser printers print a page at a time using a combination of electrostatic charges, toner, and laser light. The laser print process follows these steps:

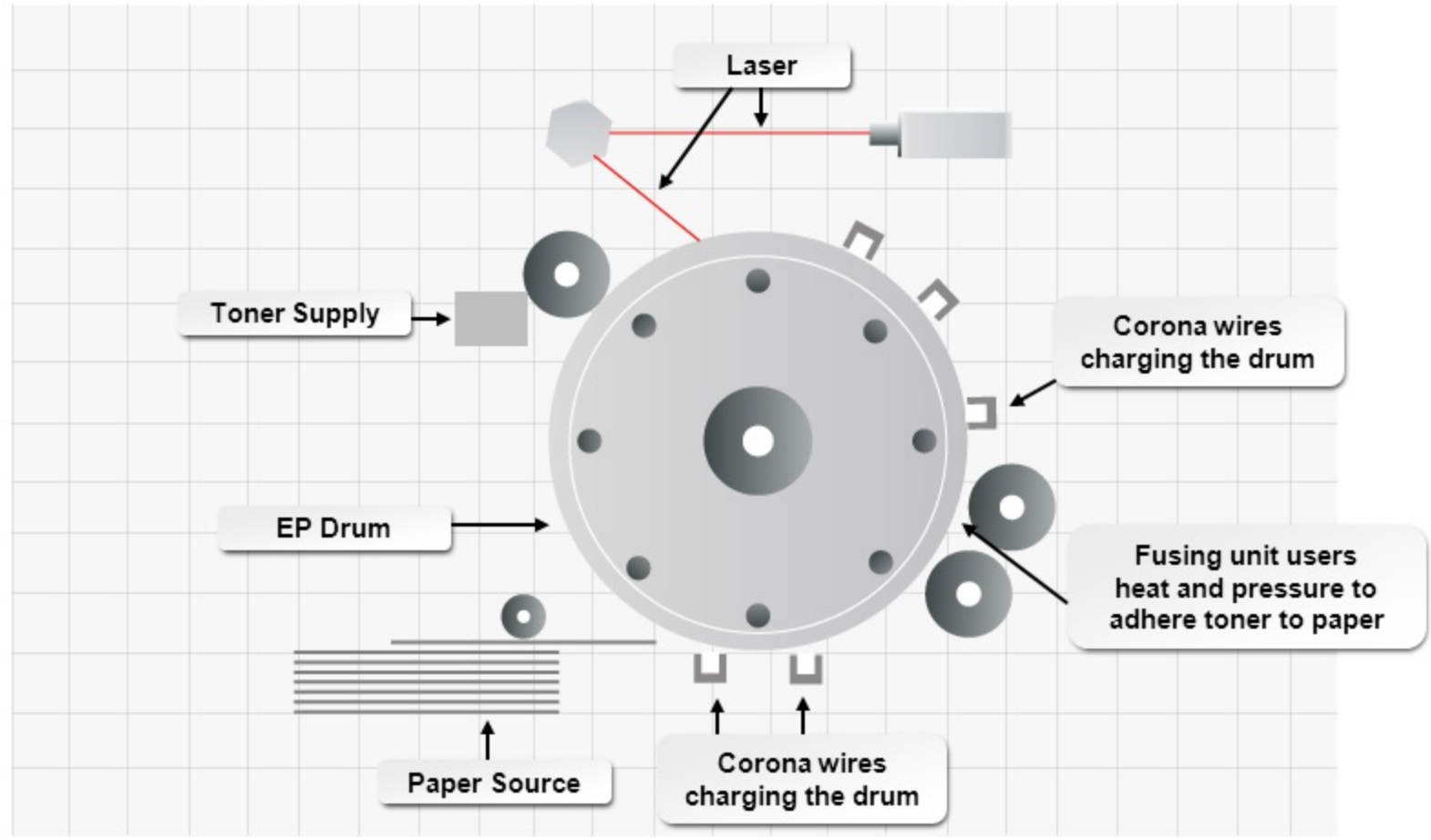

Laser
Toner Supply
Corona wires charging the drum
EP Drum
Fusing unit users heat and pressure to adhere toner to paper
Paper Source
Corona wires charging the drum

Figure: The laser print process.

Process Step	***Description***
1. Cleaning	The EP drum is cleaned with a rubber squeegee blade.
2. Erasing	Charges are removed from the EP drum in preparation for the next image.
3. Charging (conditioning)	The imaging drum is prepared by charging it with a charge roller. The roller is connected to a high-voltage power supply unit to produce negative charges. The roller then applies these negative charges, up to -600 volts (V), on the surface of the drum. This process is known as conditioning. A finely tuned laser beam, which consists of positive charges, is cast on the negatively charged drum. A multi-faced mirror that rotates reflects the laser beam onto the drum.
4. Writing	A laser beam writes to the EP drum, giving portions of the drum a weaker negative charge.
	Toner is attracted to the areas of the drum that were hit by the laser light. In this step, the invisible image is now ready to be developed. Inside the toner cartridge, a thin

5. Developing	layer of toner is applied to the surface of the drum. A thin blade, called a wipe blade, then spreads the toner evenly on the surface of the drum, leaving behind the toner only on the regions written by the laser beam.
6. Transferring	In the next phase, positively charged papers are fed into the printer by the pickup rollers. The positively charged paper attracts the negatively charged toner sticking on the drum. The transferred toner sticks loosely on the paper's surface, bound by the charges.
7. Fusing	In the final stage, the toner is melted and fused with the paper permanently. There are two transfer rollers, closely placed to each other, with almost no clearance between them. The heating roller at the top has heating elements inside it and is also coated with a non-stick material to prevent the toner from sticking to it. The pressure roller at the bottom presses the paper against the heating roller and together they melt and fuse the toner with the paper. When the fusing process is complete, the printed paper rolls out of the printer.

Inkjet Printers

An *inkjet printer* is a printer that forms images by spraying liquid ink from an ink cartridge out of nozzles aimed carefully on the printer. Inkjet printers have a self-cleaning cycle and will park the printhead when not in use. The printer can use heat or vibrations to release the ink.

Note: Canon refers to their inkjet printers as "BubbleJet," and HP refers to theirs as "DeskJet."

Figure: An inkjet printer.

Inkjet Printer Capabilities

Inkjet printers are very versatile. Inkjet printers vary by:

- The media they can print on. This includes the following:
  - Inexpensive copier paper
  - Bright paper made specifically for inkjet printers
  - Photo paper
  - Transparencies

    - Labels
    - Card stock
    - Envelopes
- Whether they produce black and white or color output.
- Whether they have duplexing capabilities.
- The cartridge design and the cost of cartridges.
- The speed at which they print.
- Whether the printhead is part of the printer or whether it is packaged together with the ink tanks in a print cartridge.
- The paper path. Some printers have a straight-through paper path and others turn the paper over as it passes through the printer.
- The resolution in dots per inch (DPI).
- How the ink is released. It could be by:
    - The piezoelectric method, used in Epson printers. This uses a vibration to release a droplet of ink from the cartridge.
    - The thermal method, used in most other printers. This method releases a droplet of ink by heating up the ink.
- The volume of the ink drop, expressed in picoliters (10^-12 liters). The smaller the drop, the less grainy the print output.

Solid Ink Printers

Solid ink printers are somewhat of a cross between inkjet and laser printers except that they use ink from melted solid-ink sticks. The melted ink is forced into a printhead, where it is transferred to a drum, which then transfers the image to the paper as it rolls over the drum. Solid ink printers can produce an image with a clear, fine edge on a wide variety of media, such as standard paper or transparency film.

The Inkjet Print Process

In the inkjet print process, inkjet printers spray ink on paper to form images. The inkjet print process follows these steps:

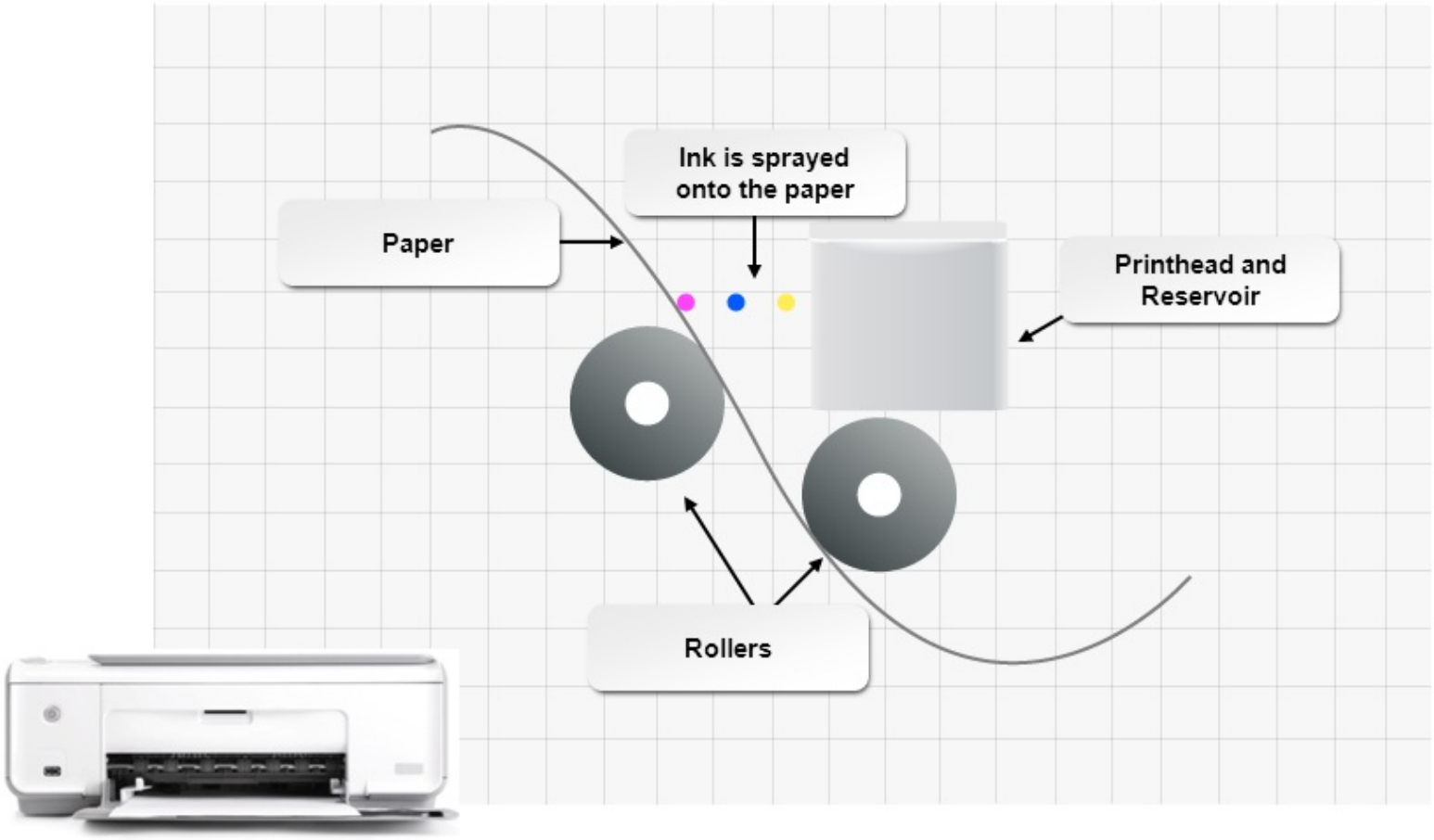


Figure: The inkjet printing process.

Process Step	***Description***
1. Preparation	When the print process is initiated, a motor and belt mechanism moves a printhead across the printer. Another stepper motor along with gears advance the paper into the printer.
2. Ink dispersion	As the printhead moves across the paper, images are formed by heat or vibration forcing liquid ink out of carefully aimed nozzles onto the paper. The printhead does not touch the paper. If the printer has double-sided printing capabilities, then the duplexing assembly will move the paper or other printing media through the printer twice.
3. Ink deposit	The printhead moves back and forth across the paper, printing one row of the image at a time. Each row is several dots wide. The amount of ink shot onto the page is determined by the driver software that controls where and when each nozzle deposits ink. The printhead typically produces at least 300 distinct DPI. Some printers can print at up to 1,200 DPI or more.

4. Paper advance	The paper advances using rollers and feeders after every row until the page is covered.

Thermal Inkjet Printers

Thermal inkjet printers use heat to release the ink from the nozzle.

1. The ink in the printhead is heated to a specified temperature.
2. Once the ink is heated, bubbles are formed in the cartridge that burst and shoot ink onto the media.
3. The heat is turned off and the element cools.
4. More ink is sucked into the nozzle when the bubble collapses. Each thermal printhead has about 300 to 600 nozzles that shoot spheres of ink that can create dots about 60 microns in diameter.

Piezoelectric Inkjet Printers

Some inkjet printers use piezoelectric technology. Piezoelectric technology uses a piezo crystal that flexes when current flows through it. When current flows to the crystal, it changes shape just enough to force a drop of ink out of the nozzle and onto the paper.

Duplexing

Duplexing is the process that enables automatic printing and scanning on both sides of printing media, such as paper and envelopes. This function can be found in both inkjet and laser printers, and also in MFDs, and in some cases can be installed as an add-on to provide the duplexing functionality to printers that do not have the function installed. The printer component that is responsible for duplexing is referred to as the *duplexing assembly*. Its primary function is to reverse the media inside the printer so that both sides can be moved through the imaging function of the printer. In some higher-end commercial printers, the duplexing function can print both sides simultaneously, without having to flip the media over.

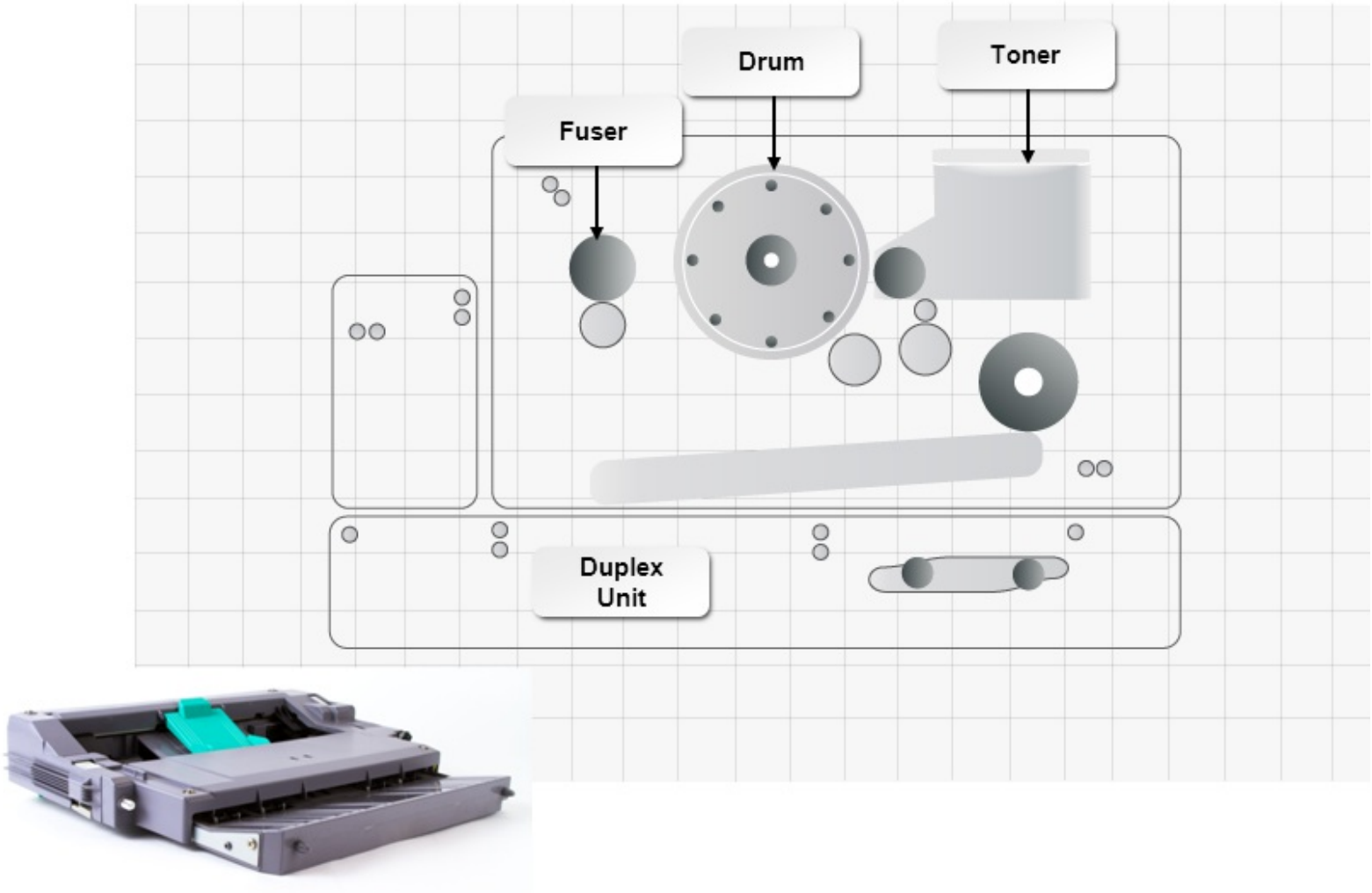


Figure: The duplexing assembly.

Thermal Printers

A *thermal printer* is a general term for any printer that uses a heating element to create the image on the paper with dye, ink from ribbons, or directly with pins while the feed assembly moves the media through the printer. There are several types of thermal printers that use significantly different technologies and are intended for different uses. The most sophisticated types of thermal printers can produce professional photo-quality images. There are also thermal printers for everyday office use and for special-purpose applications. Most thermal printers will require special *thermal paper* that contain chemicals designed to react and change color as it is heated by the heating element within the printer to create images. These printers are commonly used with cash registers to print receipts.

Figure: A thermal printer.

Types of Thermal Printers

There are three basic categories of thermal printers.

Thermal Printer Type	***Definition***
Thermal dye transfer printer	A *thermal dye transfer printer*, also called a *dye sublimation printer*, is a sophisticated type of color printer that uses heat to diffuse dye from color ribbons onto special paper or transparency stock. The resulting continuous-tone image is similar in quality to photographic printing, and professional photographers employ them to produce prints quickly without having to send them to a photographic lab. However, the printers themselves are expensive and slow, and the special media is also expensive. Newer and less-expensive *snapshot printers* produce snapshot-sized images of acceptable photographic quality.
	Thermal wax transfer printers have a thermal printhead that melts wax-based ink from a

Thermal wax transfer printer	transfer ribbon onto the paper. These printers can be used in typical office settings as an economical way to produce color copies or color prints at an acceptable quality but at lower cost than dye sublimation printers. They are also used for standard text-based printing.
Direct thermal printer	*Direct thermal* printers use heated pins to form an image directly onto specially coated thermal paper. Early personal computer printers, such as Apple's first printer, the SilenType, were thermal printers. However, direct thermal printers are found today only in special-purpose printing devices such as cash registers and some fax machines.

Thermal Print Processes

There are several different print technologies grouped together in the general category of thermal printers. Each specific thermal printer type uses a unique print process:

- A thermal dye transfer printer, or dye sublimation printer, uses a heating element to diffuse dye from color ribbons onto special thermal paper or transparency stock.
- A thermal wax transfer printer uses the heating element to melt wax-based ink from a transfer ribbon onto special thermal paper as it moves through the printer by the feed assembly.
- A direct thermal printer has a heating element with heated pins to create the image directly on the paper as it gets passed through the printer by the feed assembly.

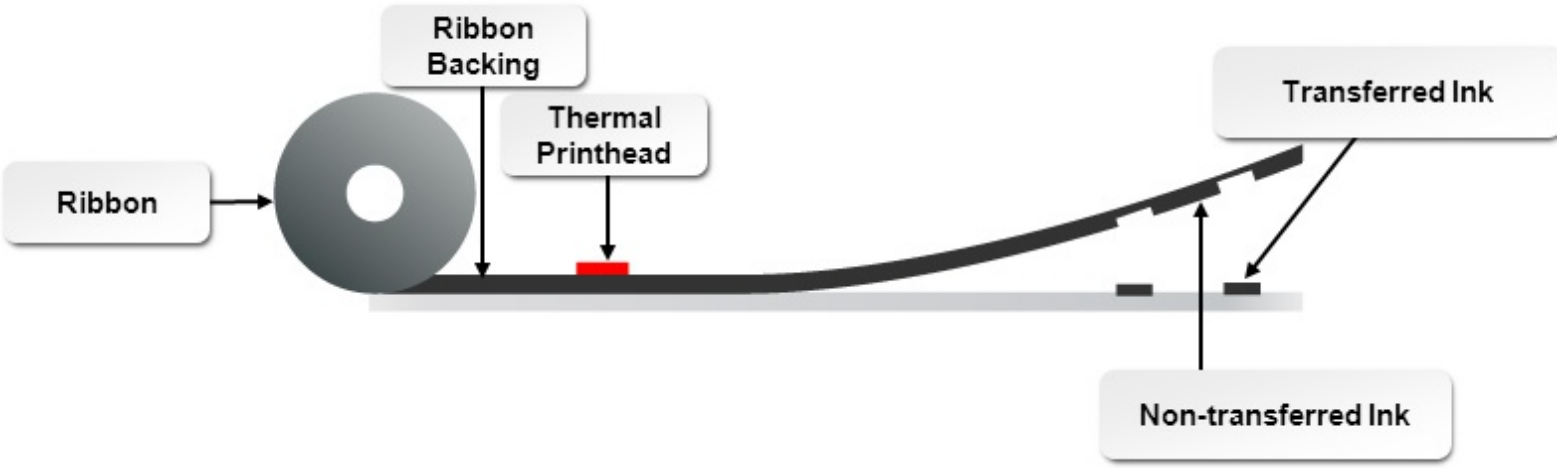


Figure: The wax thermal print process.

Impact Printers

An *impact printer* is any type of printer that strikes a component directly against the ink ribbon to create characters on impact paper. The strike can be made with a group of pins or with a preformed type character. Impact printers tend to be noisy and slow compared to other printers and have largely been superseded by other printer technologies. The most common use is for printing carbon or carbonless multi-part forms such as receipts or invoices.

Figure: An impact printer.

Types of Impact Printers

There are several terms used to categorize impact printers.

Impact Printer Type	***Description***
Dot-matrix printer	A *dot-matrix printer* is a type of impact printer that uses a set of pins to strike the ribbon. Dot-matrix printers create printed characters by using various combinations of dots. The printhead contains a vertical column of small pins that are controlled by an electromagnet. Because it uses an array of pins to form images, this type of printer can produce graphics as well as text.
Formed-character printer	A *formed-character printer* is any type of impact printer that functions like a typewriter, by pressing preformed characters against the ink ribbon to deposit the ink on the page. The printhead might be shaped like a golf ball, with the type distributed around the ball, or it might be in the form of a wheel with the characters around the perimeter of the wheel. Because of this type of printhead's resemblance to flower petals, they are referred to as

	daisy-wheel printers.
Line printer	A *line printer* is any type of impact printer that can print a full line of text at a time, rather than printing character by character. These are the fastest type of impact printers.

Paper Feed Mechanisms

Impact printers can use either tractor feed when printing on continuous-roll impact paper, or friction feed when printing on individual cut sheets of paper. Tractor feed uses pairs of wheels with pins evenly spaced around the circumference at a set spacing. Continuous-roll paper with matching holes in the edges fits over the pins. The wheels turn and pull the paper through the printer. There are usually just two wheels, but there might be additional wheels or pin guides that the paper is latched to. There is usually a lever or other setting on the printer that needs to be engaged in order to use the tractor feed.

Friction feed uses two rollers placed one on top of the other. The rollers turn to force individual cut sheets of paper or envelopes through the paper path. This is used to print on individual sheets of paper (cut-sheet paper) and envelopes. Be sure to set the printer lever or other setting to the cut-sheet mode when printing using friction feed.

The Impact Print Process

The impact print process consists of four steps.

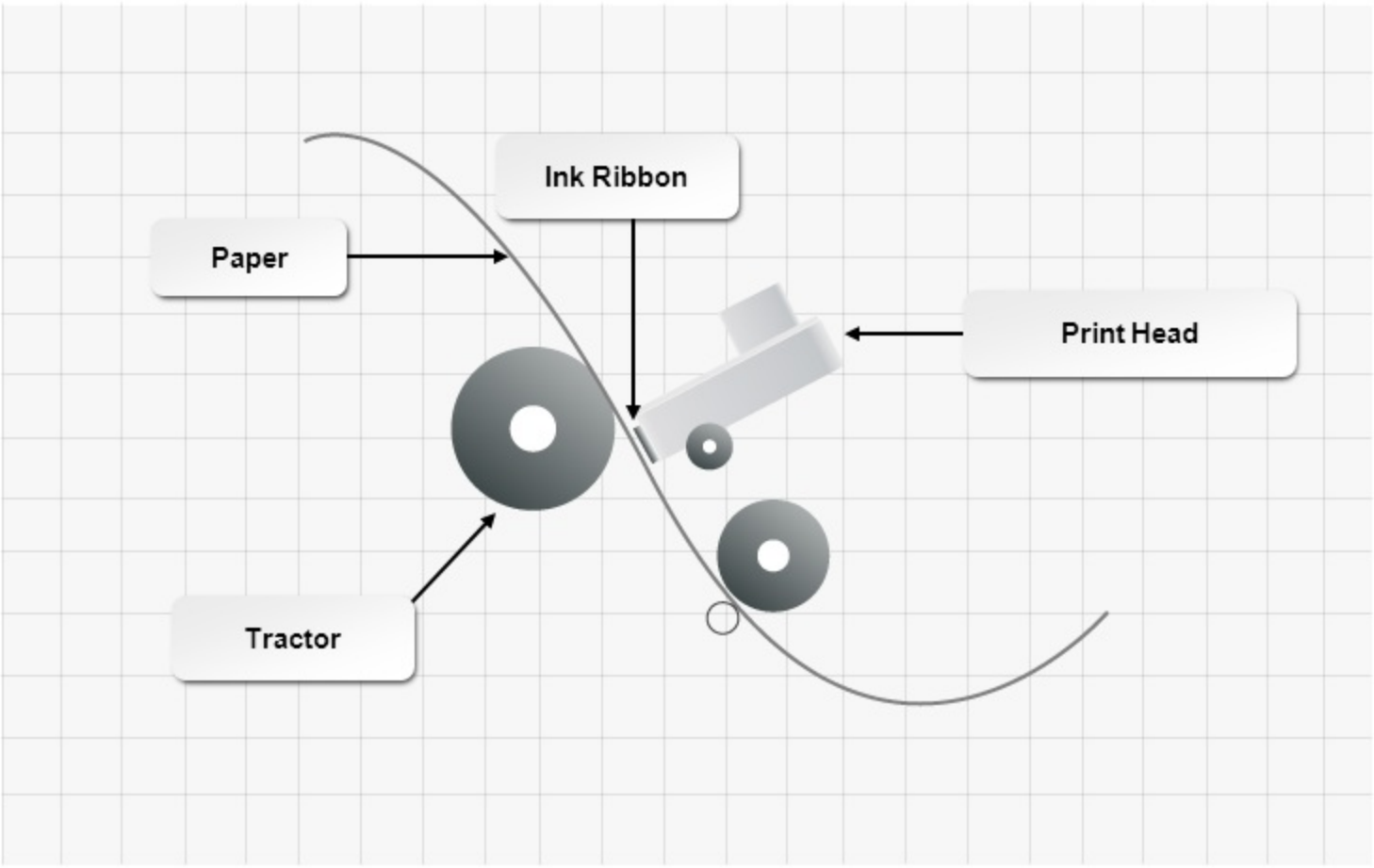


Figure: The impact print process.

Process Step	***Description***
Pin strike	The printhead has a vertical column of small pins that are controlled by an electromagnet. The pins shoot out of the printhead and strike an ink-coated ribbon. The dots created on the page become the printed text or graphics. More, smaller pins create better quality images. Printers come in 9-pin or 24-pin varieties.
Ink transfer	The impact of the pin transfers ink from the ribbon to the printed page. This physical impact is responsible for the printer's ability to print multiple-layer forms.
Printhead move	After a set of pins has fired, an electromagnet pulls them back in, the printhead moves a fraction of an inch across the page, and another set of pins is fired.
Letter quality pass	Near Letter Quality (NLQ) printers usually use two or more passes over a line of text to increase the number of dots used per letter. This connects the dots to form sharper and clearer letters.

ACTIVITY 8-1: Identifying Printer Technologies

Scenario

In this activity, you will identify various types of printers.

1. **What printer process is displayed here?**

__ Laser
__ Impact
_x_ Inkjet
__ Thermal

2. **What printer is displayed here?**

__ Inkjet
__ Thermal

__ Laser
_x_ MFD

3. **True or False? The fuser assembly is a component of a laser printer.**

_x_ True
__ False

4. Identify any available printers that may be within your workspace for taking this class. See how many of the components you can identify inside the printers.

Topic B: Install, Configure, and Maintain Printers

In the previous topic, you examined printer technologies, components, and processes. You can use this basic understanding when you install and configure printers on laptop and desktop systems. In this topic, you will install, configure, and maintain printers.

Because printers are such a fundamental component of almost every computing environment, it is almost a guarantee that you will be called upon to set up and configure printing on devices no matter what professional environment you are working in. The skills you will learn in this topic should prepare you to install, configure, and maintain a wide range of printer types efficiently and correctly.

This topic covers all or part of the following CompTIA® A+® (2012) Exam 220–801 certification objectives:

- Objective 4.2: Given a scenario, install and configure printers.
- Objective 4.3: Given a scenario, perform printer maintenance.

Technical Printer Components

Printer types can vary, but there are many common technical components that are used to provide a number of common functions within the printer.

Component	*Description*
Printer memory	Printers typically come with their own installed memory to store information about the current device settings as well as the print jobs in the queue. Different devices will have a different amount of memory installed by default; you may be able to upgrade the memory. Upgrading the memory can enable a printer to handle higher-resolution jobs and to buffer more of each print job to increase throughput. Printers store current print jobs in volatile Random Access Memory (RAM); they typically store device settings in flash-based non-volatile RAM. Consult your device documentation for the memory amounts and types your device supports, as well as procedures for installing or upgrading device memory.
Printer drivers	Like all hardware devices, printers require appropriate software drivers in order to enable the device to communicate with the computer system and function correctly. The driver controls all device-specific functions, including print resolution and quality choices, color rendition, contrast and brightness, and finishing options such as two-sided printing, collation, stapling, and so on. If you open a device's property sheet, you can see the driver functions on the **Advanced** page and on any custom pages the driver adds. Printers might also include management software that is separate from the low-level driver interface and provides sophisticated control over device settings and functions.
Printer firmware	Many printers include built-in firmware that provides the on-board device management interface. This enables you to configure printer functions, monitor and manage print jobs, select output options, and run diagnostic tests from a console on the device itself, rather than indirectly through a computer operating system. The firmware type and the functions provided by the firmware will vary depending upon your device. Check with your device vendor for any available firmware updates.
Printer interfaces	Printers have been traditionally connected to computers using parallel or sometimes serial cables and ports. However, those connection methods are considered obsolete. Most printers and multifunction devices used today use USB and wireless technologies, or are directly connected to the network via a network cable.

Centronics Ports and Connectors

One of the few places you will come across a Centronics connector is with printers. The Centronics standard describes a type of parallel port used to connect printers. It is named after the company that designed the original interface. The Centronics standard uses a 36-pin Centronics connector to connect to the printer and a DB-25 (25-pin) connector to connect to the PC.

Printer Supplies and Media

There are a number of additional printer supplies and media that are necessary for a printer to function properly.

Supply or Media	***Description***
Printer toner	Laser printer toner is a fine powder made of particles of iron, carbon, and resin. Laser printers require a toner cartridge, which is a single, replaceable unit that contains toner as well as additional components used in image production. You will need to maintain a supply of the proper toner cartridges for your printer model. Refill or recycle empty toner cartridges; do not dispose of them in regular trash. Users can change toner cartridges, but everyone should follow proper handling procedures, which are usually printed right on the cartridge. Toner particles can stain clothing or skin, especially when exposed to heat. Toner rarely spills, but when it does, clean it up with an electronics vacuum that has a fine filter and bag to contain the material. Using a regular vacuum can melt the toner if it gets on the vacuum motor. Use a dry paper towel, toner spill cloths, or cool water to clean toner from skin or clothing. Do not rub the area, because the heat from friction will make it harder to remove.
Ink and ink cartridges	Inkjet printers require ink cartridges to supply black or colored ink. You will need to maintain a supply of the ink cartridges for your printer model. Ink cartridges vary by: • The size of cartridges and how much ink each cartridge contains. • Whether black is produced using a separate cartridge or by combining the cyan, yellow, and magenta inks into a composite black output. • Whether there are separate cartridges for each color or if they are all in one unit. The black cartridge is separate on almost all printers, except for some very low-end printers. If the colors are in one unit and one color runs out, the entire cartridge needs to be replaced. Solid ink printers require you to supply solid ink sticks designed for your particular printer model.
	Depending upon your printer, you may be able to print to a variety of media types, including: • Standard-quality copier paper in a variety of form sizes, such as letter, legal, tabloid, and so on.

Paper and other media types	• Bright paper made specifically for inkjet printers. • Photo paper. • Transparencies. • Labels. • Card stock. • Envelopes. You will need to install paper trays that accommodate the media stock you select for your printer. You can also select paper trays in different orientations, whether letter or landscape. Some media sizes and types might need to be fed into the printer manually. Most printer outputs goes to an output bin on top of the printer, but there might be an additional or alternate straight paper path through a drop-down door, called a bypass tray, on the rear of the printer that you can use for specialized media, such as transparencies. Maintain an appropriate media stock on hand. Users can typically refill paper trays themselves if the correct stock is available.

Printer Driver Types

There are several types of drivers you might encounter when supporting printers. In Windows, each of these drivers is normally composed of several files. A typical driver will contain a configuration file (.dll), a driver file (.drv), a data file (.ppd), a .help file (.hlp), and one or more dependent files (.ntf).

Driver Type	***Description***
PostScript printer description (PPD)	A printer driver used to render print jobs into the PostScript printer language and provide device capability information to the user. It displays specific information about the printer itself, such as whether the printer is a color printer. It also contains options that can be modified by the user, such as paper size, resolution, and print job information. PPD files can be used on Windows®, Mac®, or LPD (Line Printer Daemon) clients.
Printer control language (PCL)	A print driver protocol used to render print jobs into the PCL printer language and transfer data from the central processing unit (CPU) to the printer. It has become a standard used mostly by Hewlett-Packard printers. This protocol can be found for laser, thermal, and dot matrix printers. Sometimes seen as Printer Command Language.
Universal print driver (UPD)	UPDs are designed to support multiple printers and MFDs with one driver. The universal drivers may only be available for some printer brands. For example, Hewlett-Packard developed a UPD that can support almost all Hewlett-Packard printers and MFDs.
Raster/bitmap	A universal driver type that supports raster/bitmap printing to most printers.
Plotter/vector	Renders print jobs into specialized plotter language, for making large-scale drawings based on X and Y coordinates.

Print Driver Compatibility

Before you can start sending print jobs to a printer, you must verify that the print driver is installed. Print drivers must be compatible with the operating system running on your computer and the type of printer you have installed. You can view the driver files for any installed printer on your system by opening the printer properties window to see the driver files in use by that printer. Print drivers are generally available on installation discs provided with the printer. Updated print drivers are usually available for download from the printer manufacturer's website. However, in most cases, the majority of print drivers will be available as part of the operating system.

Local and Network-Based Printers

There are two general types of printers you can install on a Windows system.

- *Local printers* are managed by and may be physically or wirelessly connected to the local computer. The local computer holds the *print queue*, which contains the print jobs waiting to print.

- *Network-based printers* are shared print devices that are managed by a network computer, called a *print server*. The print server holds the print queue.

  Network-connected printers have built-in network adapter cards and connect directly to a network cable or via a wireless network interface. Print jobs are sent over the network using a network protocol such as Transmission Control Protocol/Internet Protocol (TCP/IP). Some network-connected printers have on-board print server software so they can be installed on the network directly and manage the print queue without requiring a separate print server computer.

Print Device Sharing

Depending on an organization's infrastructure, printers can be shared with computers, networks, or other devices using a number of methods. Both local and network printers can be shared with other computers and devices.

Method	*Description*
Wired	With the increased use of USB and Ethernet cables over the years, parallel and serial cables and ports are just about obsolete. Most wired printers and MFDs found today will connect to devices using a USB port or are directly connected to a network via an Ethernet cable.
Wireless	Wireless printers offer many capabilities such as flexible printer locations. Printers can be connected to a wireless network using: • Bluetooth® • 802.11x • Infrared (IR) technology
Print server	Print servers hold the print queue for a number of printers connected to the same network. The server manages print jobs that come from client computers or devices, and sends the jobs on to the desired printer. You may also come across occasions when the print server is built into a printer, or is a component of an appliance that also provides additional functions, such as a firewall.
Operating system	Printers can be shared with other devices on the network by assigning print permissions that apply to local users and to users of a shared network printer. Permissions can be allowed or denied within the operating system settings, but if you deny a user the print permission, the user will have no access to the printer. Available permissions include: • The print permission, which enables you to print to the shared printer. Assigned by default to Everyone. • Manage this printer, which enables you to print to the printer and fully administer the printer. Assigned by default to administrators and Power Users. • Manage documents, which enables you to manage other users' documents. This permission includes the ability to manage all the jobs in the print queue. • Special permissions, which is generally only used by the system administrator to manage printer owner settings.

Workgroup Security Models and Print Permissions

To assign permissions to printer objects on a Windows® 7 computer in a workgroup, you need to turn off **File Sharing** and enable **Classic authentication** so that local users can authenticate as themselves. In the **Network and Sharing Center,** select **Change advanced sharing settings** from the left pane and then select the **Turn on file and printer sharing** option.

Note: In Windows® XP, use Simple File Sharing to change the share permissions.

Once you do this, the **Security** tab will be available in the printer's property sheet.

Printer Configuration Options

Depending upon your particular printer, you will have various options for configuring and optimizing printer performance.

Printer Configuration Option	***Description***
Device calibration	The printer manufacturer should provide documentation and tools for calibrating device-specific settings on the physical print device. For example, the cartridges on inkjet printers often require alignment after changing the cartridge (this often happens automatically, or may be done manually through the print driver interface). Or, you may need to calibrate the color overlays so that the colors align properly and do not create shadows.
Tray assignments	Each physical printer has different numbers and sizes of media and paper trays that can accommodate different paper and media forms and weights. Once you have installed the appropriate paper trays, you should verify that the appropriate media form type is assigned to each tray. Configure form-to-tray assignments on the **Device Settings** page of the printer's property sheet.
Tray switching	If you have installed multiple trays that use the same media size and type, most printers can use automatic tray switching to switch a job to a different tray when the default tray is empty. See your printer's documentation for information on configuring tray switching.
Print spool settings	You can configure how an individual printer will spool print jobs. The printer can print as soon as a page is spooled, or it can hold the job until the entire document is spooled. You can also configure the printer to bypass spooling and print directly to the device. Set spooler options on the **Advanced** tab of the printer's property sheet.
Printer availability	You can use the printer's availability schedule to postpone printing of long documents or low-priority documents to off-hours or other convenient times. Users can send jobs to the print queue at all times; the print server holds the jobs until the available hours, and then produces the output. To configure availability, open the properties of the printer and select the **Advanced** tab. Select **Available From** and set the time range in the boxes.
Color management	The settings on the **Color Management** page control how Windows will select color settings for the printer based on the media type and printer configuration.
Printer ports	You can use the **Ports** tab to configure the printer to print to local parallel or serial ports, or to a network port address.

LearnTO: For additional information, check out LearnTO **Install and Configure a Printer** from the **LearnTO** tile for this course on your LogicalCHOICE Course screen.

Printer Maintenance

Proper printer maintenance will extend the life of a printer and will help prevent mechanical issues in the future.

Device	*Maintenance*
Inkjet printer	• Use the printer often to prevent the ink from drying out and clogging the nozzles. • Run the printer's cleaning utility to clean the printhead. • Run the printer's nozzle test.
Impact printer	• Regularly clean the paper path and the ribbon path using a dry, soft cloth. • Replace the printhead, ribbon, and paper when needed. • Regularly vacuum the dust from the wheels in the tractor feed assembly. • To avoid overheating the printhead, be mindful of the printer's location. Make sure it is clear of clutter and other machines.
Laser printer	• Replace the toner cartridge once it gets low. • Clean excess toner out of the printer each time you replace the cartridge to avoid buildup inside the printer. • Be mindful of the printer's location. Keep it well ventilated with proper spacing from other devices.
Thermal printer	• Replace the paper when needed. • The heating element may need cleaning to prevent buildup and smudging. • Remove debris from inside and outside printer to prevent unwanted particles from getting into the printer components.

Access the Checklist tile on your LogicalCHOICE course screen for reference information and job aids on **How to Install, Configure, and Maintain Printers**

ACTIVITY 8-2: Installing and Sharing a Local Printer

Scenario

One of your clients has just asked you to install a refurbished printer that he purchased online. He would like to use this printer on his Windows 7 computer as his default printer. He has also asked that you make the printer available to other users in the company. Even though your client has not yet received the printer, he would like you to configure his computer so that all he will need to do is plug in the printer when it arrives.

1. Install the printer on your workstation.
    a. Select **Start→Control Panel.**
    b. Under **Hardware and Sound,** select **View devices and printers.**
    c. Select **Add a printer** and then select **Add a local printer.**
    d. From the **Use an existing port** drop-down list, select **USB001 (Virtual printer port for USB), LPT1** or **LPT2,** and then select **Next.**
    e. On the **Install the printer driver** page, from the **Manufacturer** list, select a printer manufacturer.
    f. From the **Printers** list, select a printer and select **Next.**
    g. In the **Printer name** text box, type ***My Local Printer***
    h. Select **Next.**
    i. Select **Finish,** and close the **Devices and Printers** window.
2. Share the printer.
    a. Open the **Control Panel.**
    b. Under **Network and Internet,** select **Choose homegroup and sharing options.**
    c. Select the **Change advanced sharing settings** link.
    d. Under the **File and printer sharing** section, select the **Turn on file and printer sharing** option and then select **Save changes.**
    e. Close the **Advanced sharing settings** window.
3. Create a print job on the local printer.
    a. Open the **Control Panel.**
    b. Under **Hardware and Sound,** select **View devices and printers.**
    c. Display the pop-up menu for **My Printer** and select **Printer properties.**
    d. Select **Print Test Page.**
    e. Select **Close.**
    f. Select **OK.**
    g. Select **See what's printing.**
    h. At least one print job should appear in the queue. Close the print queue window and the **Devices and Printers** window.

Summary

In this lesson, you supported printers. Because printers enable users to transfer digital information to paper, they are among the most commonly used devices in almost every type of computing environment. As an A+ certified professional, you can use the skills and knowledge from this lesson when you are called upon to install, configure, or troubleshoot printers

What types of printer have you had experience with in your current job role?

In your experience, what printer maintenance tasks are you most familiar with?

Social: Check your LogicalCHOICE Course screen for opportunities to interact with your classmates, peers, and the larger LogicalCHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

Course Summary

Congratulations! You have completed the CompTIA® A+® Certification Exam 220-801 course. You have acquired the essential skills and information you will need to install, upgrade, configure, and perform preventative maintenance of basic PC hardware. If you are getting ready for a career as an entry-level IT professional or PC service technician, and if your job duties will include any type of PC service tasks or technical support for computer users, this course has provided you with the background knowledge and skills you will require to be successful. Completing this course is also an important part of your preparation for the CompTIA A+ certification examination (220-801) that you must pass in order to become a CompTIA A+ Certified Professional.

What's Next?

If you are preparing for the CompTIA A+ certification, you will also need to take and pass the CompTIA A+ 220-802 exam. You should plan on attending the Logical Operations CompTIA A+ Certification Exam 220-802 course. This course focuses on the skills needed to support operating systems; create secure computing environments; support mobile devices; and troubleshoot issues related to hardware, operating systems, networks, security, laptops, mobile devices, and printers.

If you want to learn more about networking technologies and supporting network users, you might want to attend the Logical Operations CompTIA® Network+® (Exam N10-005) course. If you want to learn more about security and helping users use safe computing practices, you might want to attend the Logical Operations CompTIA® Security+® (Exam SY0-301) course.

You are encouraged to explore PC and network support further by actively participating in any of the social media forums set up by your instructor or training administrator through the **Social Media** tile on the LogicalCHOICE Course screen.

Appendix A: Mapping Course Content to CompTIA® A+® Exam 220-801

Obtaining CompTIA A+ certification requires candidates to pass two examinations. This table describes where the objectives for CompTIA exam 220-801 are covered in this course.

Domain and Objective	*Covered In*
1.0 PC Hardware	
1.1 Configure and apply BIOS settings.	
• Install firmware upgrades – flash BIOS	Lesson 1, Topic A

• BIOS component information
  • RAM
  • Hard drive
  • Optical drive
  • CPU
	Lesson 4, Topic F

• BIOS configurations
  • Boot sequence
  • Enabling and disabling devices
  • Date/time
  • Clock speeds
  • Virtualization support
	Lesson 4, Topic F

• BIOS security (passwords, drive encryption: TPM, lo-jack)	Lesson 4, Topic F
• Use built-in diagnostics	Lesson 4, Topic F

• Monitoring
  • Temperature monitoring
  • Fan speeds
  • Intrusion detection/notification
  • Voltage
  • Clock
  • Bus speed
	Lesson 4, Topic F

1.2 Differentiate between motherboard components, their purposes, and properties.	

• Sizes
  • ATX
  • Micro-ATX
  • ITX
	Lesson 4, Topic A

• Expansion slots
  • PCI
  • PCI-X
  • PCIe
  • miniPCI
  • CNR
  • AGP2x, 4x, 8x
	Lesson 4, Topic A

• RAM slots	Lesson 4, Topic A
• CPU sockets	Lesson 4, Topic B

• Chipsets
  • North Bridge
  • South Bridge
  • CMOS battery
	Lesson 4, Topic A

• Jumpers	Lesson 4, Topic A
• Power connections and types	Lesson 4, Topic A
• Fan connectors	Lesson 4, Topic A

• Front panel connectors
  • USB
  • Audio
  • Power button
  • Power light
  • Drive activity lights
	Lesson 4, Topic A

• Reset button	
• Bus speeds	Lesson 4, Topic A
1.3 Compare and contrast RAM types and features.	

• Types
  • DDR
  • DDR2
  • DDR3
  • SDRAM
  • SODIMM
  • RAMBUS
  • DIMM
  • Parity vs. non-parity
  • ECC vs. non-ECC
  • RAM configurations
	Lesson 4, Topics A and D; Lesson 7, Topic A

• Single channel vs. dual channel vs. triple channel • Single sided vs. double sided	Lesson 4, Topic D
• RAM compatibility and speed	Lesson 4, Topic D
1.4 Install and configure expansion cards.	
• Sound cards	Lesson 3, Topic C
• Video cards	Lesson 3, Topic C

• Network cards	Lesson 3, Topic C
• Serial and parallel cards	Lesson 3, Topic C
• USB cards	Lesson 3, Topic C
• FireWire cards	Lesson 3, Topic C
• Storage cards	Lesson 3, Topic C
• Modem cards	Lesson 3, Topic C
• Wireless/cellular cards	Lesson 3, Topic C
• TV tuner cards	Lesson 3, Topic C
• Video capture cards	Lesson 3, Topic C
• Riser cards	Lesson 3, Topic C
1.5 Install and configure storage devices and use appropriate media.	

• Optical drives
  • CD-ROM
  • DVD-ROM
  • Blu-ray
	Lesson 1, Topic B; Lesson 4, Topic E

• Combo drives and burners
  • CD-RW
  • DVD-RW
  • Dual Layer DVD-RW
  • BD-R
  • BD-RE
	Lesson 1, Topic B

• Connection types
  • External (USB, FireWire, eSATA, Ethernet)
  • Internal SATA, IDE and SCSI [IDE configuration and setup (Master, Slave, Cable Select), SCSI IDs (0 – 15)]
  • Hot swappable drives
	Lesson 1, Topic B; Lesson 4, Topic E

• Hard drives
  • Magnetic
  • 5400 rpm
  • 7200 rpm
  • 10,000 rpm
  • 15,000 rpm
	Lesson 1, Topic B

• Solid state/flash drives
  • Compact flash
  • SD
  • Micro-SD
  • Mini-SD
  • xD
  • SSD
	Lesson 1, Topic B; Lesson 4, Topic E

• RAID types
  • 0
  • 1
  • 5
  • 10
	Lesson 4, Topic E

• Floppy drive	Lesson 1, Topic B; Lesson 4, Topic E
• Tape drive	Lesson 1, Topic B; Lesson 4, Topic E

• Media capacity
  • CD
  • CD-RW
  • DVD-RW
  • DVD
  • Blu-Ray
  • Tape
  • Floppy
	Lesson 4, Topic E

• DL DVD	
1.6 Differentiate among various CPU types and features and select the appropriate cooling method.	

• Socket types
  • Intel: LGA, 775, 1155, 1156, 1366
  • AMD: 940, AM2, AM2+, AM3, AM3+, FM1, F
	Lesson 4, Topic B

• Characteristics
  • Speeds
  • Cores
  • Cache size/type
  • Hyperthreading
  • Virtualization support
  • Architecture (32-bit vs. 64-bit)
  • Integrated GPU
	Lesson 4, Topic B

• Cooling
  • Heat sink
  • Fans
  • Thermal paste
  • Liquid-based
	Lesson 4, Topic B

1.7 Compare and contrast various connection interfaces and explain their purpose.	

• Physical connections
  • USB 1.1 vs. 2.0 vs. 3.0 speed and distance characteristics (Connector types: A, B, mini, micro)
  • FireWire 400 vs. FireWire 800 speed and distance characteristics
  • SATA1 vs. SATA2 vs. SATA3, eSATA, IDE speeds
  • Other connector types (Serial, Parallel, VGA, HDMI, DVI, audio, RJ-45, RJ-11)
  • Analog vs. digital transmission (VGA vs. HDMI)
	Lesson 1, Topic B; Lesson 1, Topic C; Lesson 6, Topic A

• Speeds, distances and frequencies of wireless device connections • Bluetooth	

• IR • RF	Lesson 1, Topic C
1.8 Install an appropriate power supply based on a given scenario.	

• Connector types and their voltages
  • SATA
  • Molex
  • 4/8-pin 12v
  • PCIe 6/8-pin
  • 20-pin
  • 24-pin
  • Floppy
	Lesson 4, Topic C

• Specifications
  • Wattage
  • Size
  • Number of connectors
  • ATX
  • Micro-ATX
	Lesson 4, Topic C

• Dual voltage options	Lesson 4, Topic C
1.9 Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs.	

• Graphic / CAD / CAM design workstation
  • Powerful processor
  • High-end video
  • Maximum RAM
	Lesson 5, Topic B

• Audio/Video editing workstation
  • Specialized audio and video card
  • Large fast hard drive
  • Dual monitors
	Lesson 5, Topic B

• Virtualization workstation • Maximum RAM and CPU cores	Lesson 5, Topic A

• Gaming PC
  • Powerful processor
  • High-end video/specialized GPU
  • Better sound card
  • High-end cooling
	Lesson 5, Topic B

• Home Theater PC
  • Surround sound audio
  • HDMI output
  • HTPC compact form factor
  • TV tuner
	Lesson 5, Topic B

• Standard thick client
  • Desktop applications
  • Meets recommended requirements for running Windows
	Lesson 5, Topic A

• Thin client
  • Basic applications
  • Meets minimum requirements for running Windows
	Lesson 5, Topic A

• Home Server PC
  • Media streaming
  • File sharing
  • Print sharing
  • Gigabit NIC
  • RAID array
	Lesson 5, Topic B

1.10 Given a scenario, evaluate types and features of display devices.	

• Types
  • CRT
  • LCD
  • LED
  • Plasma
  • Projector
  • OLED
	Lesson 3, Topic A

• Refresh rates	Lesson 3, Topic A
• Resolution	Lesson 3, Topic A
• Native resolution	Lesson 3, Topic A
• Brightness/lumens	Lesson 3, Topic A
• Analog vs. digital	Lesson 3, Topic A
• Privacy/antiglare filters	Lesson 3, Topic A
• Multiple displays	Lesson 3, Topic A
1.11 Identify connector types and associated cables.	

• Display connector types
  • DVI-D
  • DVI-I
  • DVI-A
  • Display Port
  • RCA
  • DB-15
  • BNC
  • mini-HDMI
  • RJ-45
  • Din-6
	Lesson 1, Topic C; Lesson 6, Topic A

• Display cable types
  • HDMI
  • DVI
  • VGA
  • Component
  • Composite
  • S-video
  • RGB
	Lesson 1, Topic C

• Coaxial • Ethernet	

• Device connectors and various connector pin-outs
  • SATA
  • eSATA
  • PATA (IDE and EIDE)
  • Floppy
  • USB
  • IEEE1394
  • SCSI
  • PS/2
  • Parallel
  • Serial
  • Audio
  • RJ-45
	Lesson 1, Topic C; Lesson 6, Topic A

• Device cable types
  • SATA
  • eSATA
  • IDE
  • EIDE
  • Floppy
  • USB
  • IEEE1394
  • SCSI (68pin vs. 50pin vs. 25pin)
  • Parallel
  • Serial
  • Ethernet
  • Phone
	Lesson 1, Topic C; Lesson 6, Topic A

1.12 Install and configure various peripheral devices.	

• Input devices
  • Mouse
  • Keyboard
  • Touch screen
  • Scanner
  • Barcode reader
  • KVM
  • Microphone
  • Biometric devices
	Lesson 3, Topic B

• Game pads • Joysticks • Digitizer	

• Multimedia devices
  • Digital cameras
  • Microphone
  • Webcam
  • Camcorder
  • MIDI enabled devices
	Lesson 3, Topic D

• Output devices
  • Printers
  • Speakers
  • Display devices
	Lesson 1, Topic B; Lesson 3, Topics A and D

2.0 Networking	
2.1 Identify types of network cables and connectors.	
• Fiber • Connectors: SC, ST and LC	Lesson 6, Topic A

• Twisted Pair
  • Connectors: RJ-11, RJ-45
  • Wiring standards: T568A, T568B
	Lesson 6, Topic A

• Coaxial • Connectors: BNC, F-connector	Lesson 6, Topic A
2.2 Categorize characteristics of connectors and cabling.	

• Fiber
  • Types (single-mode vs. multi-mode)
  • Speed and transmission limitations
	Lesson 6, Topic A

• Twisted pair
  • Types: STP, UTP, CAT3, CAT5, CAT5e, CAT6, plenum, PVC
  • Speed and transmission limitations
	Lesson 6, Topic A

• Coaxial
  • Types: RG-6, RG-59
  • Speed and transmission limitations
	Lesson 6, Topic A

2.3 Explain properties and characteristics of TCP/IP.	

• IP class
  • Class A
  • Class B
  • Class C
	Lesson 6, Topic B

• IPv4 vs. IPv6	Lesson 6, Topic B
• Public vs. private vs. APIPA	Lesson 6, Topic B
• Static vs. dynamic	Lesson 6, Topic B
• Client-side DNS	Lesson 6, Topic B
• DHCP	Lesson 6, Topic B
• Subnet mask	Lesson 6, Topic B
• Gateway	Lesson 6, Topic B
2.4 Explain common TCP and UDP ports, protocols, and their purpose.	

• Ports
  • 21 – FTP
  • 23 – TELNET	

• 25 – SMTP • 53 – DNS • 80 – HTTP • 110 – POP3 • 143 – IMAP • 443 – HTTPS • 3389 – RDP	Lesson 6, Topic D

• Protocols
  • DHCP
  • DNS
  • LDAP
  • SNMP
  • SMB
  • SSH
  • SFTP
	Lesson 6, Topic D

• TCP vs. UDP	Lesson 6, Topic D
2.5 Compare and contrast wireless networking standards and encryption types.	

• Standards
  • 802.11 a/b/g/n
  • Speeds, distances and frequencies
	Lesson 6, Topic G

• Encryption types • WEP, WPA, WPA2, TKIP, AES	Lesson 6, Topic G
2.6 Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.	
• MAC filtering	Lesson 6, Topic G
• Channels (1 – 11)	Lesson 6, Topic G
• Port forwarding, port triggering	Lesson 6, Topic G

• SSID broadcast (on/off)	Lesson 6, Topic G
• Wireless encryption	Lesson 6, Topic G
• Firewall	Lesson 6, Topic G
• DHCP (on/off)	Lesson 6, Topic G
• DMZ	Lesson 6, Topic G
• NAT	Lesson 6, Topic G
• WPS	Lesson 6, Topic G
• Basic QoS	Lesson 6, Topic G
2.7 Compare and contrast Internet connection types and features.	
• Cable	Lesson 6, Topic C
• DSL	Lesson 6, Topic C
• Dial-up	Lesson 6, Topic C
• Fiber	Lesson 6, Topic C
• Satellite	Lesson 6, Topic C
• ISDN	Lesson 6, Topic C

• Cellular (mobile hotspot)	Lesson 6, Topic C
• Line of sight wireless internet service	Lesson 6, Topic C
• WiMAX	Lesson 6, Topic C
2.8 Identify various types of networks.	
• LAN	Lesson 6, Topic C
• WAN	Lesson 6, Topic C
• PAN	Lesson 6, Topic C
• MAN	Lesson 6, Topic C

• Topologies
  • Mesh
  • Ring
  • Bus
  • Star
  • Hybrid
	Lesson 6, Topic C

2.9 Compare and contrast network devices their functions and features.	
• Hub	Lesson 6, Topic C
• Switch	Lesson 6, Topic C
• Router	Lesson 6, Topic C
• Access point	Lesson 6, Topic C

• Bridge	Lesson 6, Topic C
• Modem	Lesson 6, Topic C
• NAS	Lesson 6, Topic C
• Firewall	Lesson 6, Topic C
• VoIP phones	Lesson 6, Topic C
• Internet appliance	Lesson 6, Topic C
2.10 Given a scenario, use appropriate networking tools.	
• Crimper	Lesson 6, Topic F
• Multimeter	Lesson 6, Topic F
• Toner probe	Lesson 6, Topic F
• Cable tester	Lesson 6, Topic F
• Loopback plug	Lesson 6, Topic F
• Punchdown tool	Lesson 6, Topic F
3.0 Laptops	
3.1 Install and configure laptop hardware and components.	
• Expansion options • Express card /34	

• Express card /54 • PCMCIA • SODIMM • Flash	Lesson 7, Topic A

• Hardware/device replacement
  • Keyboard
  • Hard Drive (2.5 vs. 3.5)
  • Memory
  • Optical drive
  • Wireless card
  • Mini-PCIe
  • screen
  • DC jack
  • Battery
  • Touchpad
  • Plastics
  • Speaker
  • System board
  • CPU
	Lesson 7, Topic B

3.2 Compare and contrast the components within the display of a laptop.	

• Types
  • LCD
  • LED
  • OLED
  • Plasma
	Lesson 7, Topic A

• Wi-Fi antenna connector/placement	Lesson 7, Topic A
• Inverter and its function	Lesson 7, Topic A
• Backlight	Lesson 7, Topic A
3.3 Compare and contrast laptop features.	

• Special function keys
  • Dual displays
  • Wireless (on/off)
  • Volume settings
  • Screen brightness
  • Bluetooth (on/off)
  • Keyboard backlight
	Lesson 7, Topic A

• Docking station vs. port replicator	Lesson 7, Topic A
• Physical laptop lock and cable lock	Lesson 7, Topic A
4.0 Printers	
4.1 Explain the differences between the various printer types and summarize the associated imaging process.	

• Laser
  • Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly
  • Imaging process: processing, charging, exposing, developing, transferring, fusing and cleaning
	Lesson 8, Topic A

• Inkjet
  • Ink cartridge, printhead, roller, feeder, duplexing assembly, carriage and belt
  • Calibration
	Lesson 8, Topic A

• Thermal
  • Feed assembly, heating element
  • Special thermal paper
	Lesson 8, Topic A

• Impact
  • Printhead, ribbon, tractor feed
  • Impact paper
	Lesson 8, Topic A

4.2 Given a scenario, install, and configure printers.	

• Use appropriate printer drivers for a given operating system	Lesson 8, Topic B

• Print device sharing
  • Wired (USB, Parallel, Serial, Ethernet)
  • Wireless [Bluetooth, 802.11x, Infrared (IR)]
  • Printer hardware print server
	Lesson 8, Topic B

• Printer sharing • Sharing local/networked printer via Operating System settings	Lesson 8, Topic B
4.3 Given a scenario, perform printer maintenance.	
• Laser • Replacing toner, applying maintenance kit, calibration, cleaning	Lesson 8, Topic B
• Thermal • Replace paper, clean heating element, remove debris	Lesson 8, Topic B
• Impact • Replace ribbon, replace printhead, replace paper	Lesson 8, Topic B
5.0 Operational Procedures	
5.1 Given a scenario, use appropriate safety procedures.	
• ESD straps	Lesson 2, Topic B
• ESD mats	Lesson 2, Topic B
• Self-grounding	Lesson 2, Topic B
• Equipment grounding	Lesson 2, Topic B

• Personal safety
  • Disconnect power before repairing PC
  • Remove jewelry
  • Lifting techniques
  • Weight limitations
  • Electrical fire safety
  • CRT safety – proper disposal
  • Cable management
	Lesson 2, Topics B and C

• Compliance with local government regulations	Lesson 2, Topic A
5.2 Explain environmental impacts and the purpose of environmental controls.	
• MSDS documentation for handling and disposal	Lesson 2, Topic C
• Temperature, humidity level awareness and proper ventilation	Lesson 2, Topic C

• Power surges, brownouts, blackouts
  • Battery backup
  • Surge suppressor
	Lesson 2, Topic C

• Protection from airborne particles
  • Enclosures
  • Air filters
	Lesson 2, Topic C

• Dust and debris
  • Compressed air
  • Vacuums
	Lesson 2, Topic C

• Component handling and protection • Antistatic bags	Lesson 2, Topic C
• Compliance to local government regulations	Lesson 2, Topic A

5.3 Given a scenario, demonstrate proper communication and professionalism.	
• Use proper language – avoid jargon, acronyms, slang when applicable	Lesson 2, Topic D
• Maintain a positive attitude	Lesson 2, Topic D
• Listen and do not interrupt the customer	Lesson 2, Topic D
• Be culturally sensitive	Lesson 2, Topic D
• Be on time (if late contact the customer)	Lesson 2, Topic D

• Avoid distractions
  • Personal calls
  • Talking to co-workers while interacting with customers
  • Personal interruptions
	Lesson 2, Topic D

• Dealing with difficult customer or situation
  • Avoid arguing with customers and/or being defensive
  • Do not minimize customer's problems
  • Avoid being judgmental
  • Clarify customer statements (ask open ended questions to narrow the scope of the problem, restate the issue or question to verify understanding)
	Lesson 2, Topic D

• Set and meet expectations/timeline and communicate status with the customer
  • Offer different repair/replacement options if applicable
  • Provide proper documentation on the services provided
  • Follow up with customer/user at a later date to verify satisfaction
	Lesson 2, Topic D

• Deal appropriately with customers confidential materials • Located on a computer, desktop, printer, etc	Lesson 2, Topic D

5.4 Explain the fundamentals of dealing with prohibited content/activity.	

• First response
  • Identify
  • Report through proper channels
  • Data/device preservation
	Lesson 2, Topic D

• Use of documentation/documentation changes	Lesson 2, Topic D
• Chain of custody • Tracking of evidence/documenting process	Lesson 2, Topic D
• Anti-spyware	Lesson 2, Topic E

Appendix B: CompTIA A+ Acronyms

The following table lists the acronyms that appear on the CompTIA A+ exams. Candidates are encouraged to review this list and have a working knowledge of the acronyms and their associated terms, as a part of a comprehensive exam preparation program.

Acronym	*Associated Term*
AC	alternating current
ACL	access control list
ACPI	Advanced Configuration Power Interface
ACT	activity
ADSL	Asymmetrical Digital Subscriber Line
AGP	Accelerated Graphics Port
AMD	Advanced Micro Devices
APIPA	Automatic Private Internet Protocol Addressing
APM	advanced power management
ARP	Address Resolution Protocol
ASR	automated system recovery
ATA	Advanced Technology Attachment
ATAPI	Advanced Technology Attachment Packet Interface
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology eXtended
A/V	Audio Video
BIOS	basic input/output system
BNC	Bayonet-Neill-Concelman or British Naval Connector
BTX	Balanced Technology eXtended
CAPTCHA	Completely Automated Public Turing Test To Tell Computers and Humans Apart
CCFL	Cold Cathode Fluorescent Lamp
CD	compact disc
CD-ROM	compact disc-read-only memory
CD-RW	compact disc-rewritable
CDFS	compact disc file system
CFS	Central File System, Common File System, or Command File System
CMOS	complementary metal-oxide semiconductor
CNR	Communications and Networking Riser
COMx	communication port (x=port number)
CPU	central processing unit
CRIMM	Continuity Rambus Inline Memory Mode
CRT	cathode-ray tube

DAC	discretionary access control
DB-25	serial communications D-shell connector, 25 pins
DB-9	9-pin D-shell connector
DC	direct current
DDOS	distributed denial of service
DDR	double data-rate
DDR RAM	double data-rate random access memory
DDR SDRAM	double data-rate synchronous dynamic random access memory
DFS	distributed file system
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DIN	Deutsche Industrie Norm
DIP	dual inline package
DLT	digital linear tape
DLP	digital light processing
DMA	direct memory access
DMZ	demilitarized zone
DNS	Domain Name Service or domain name server
DOS	denial of service
DRAM	dynamic random access memory
DSL	digital subscriber line
DVD	digital video disc or digital versatile disc
DVD-RAM	digital video disc-random access memory
DVD-ROM	digital video disc-read only memory
DVD-R	digital video disc-recordable
DVD-RW	digital video disc-rewritable
DVI	digital visual interface
ECC	error correction code
ECP	extended capabilities port
EEPROM	electrically erasable programmable read-only memory
EFS	encrypting file system
EIDE	enhanced integrated drive electronics
EMI	electromagnetic interference
EMP	electromagnetic pulse
EPROM	erasable programmable read-only memory
EPP	enhanced parallel port
ERD	emergency repair disk
ESD	electrostatic discharge
EVGA	extended video graphics adapter/array
EVDO	evolution data optimized or evolution data only

FAT	file allocation table
FAT12	12-bit file allocation table
FAT16	16-bit file allocation table
FAT32	32-bit file allocation table
FDD	floppy disk drive
Fn	Function (referring to the function key on a laptop)
FPM	fast page-mode
FRU	field replaceable unit
FSB	Front Side Bus
FTP	File Transfer Protocol
FQDN	fully qualified domain name
Gb	gigabit
GB	gigabyte
GDI	graphics device interface
GHz	gigahertz
GUI	graphical user interface
GPS	global positioning system
GSM	global system for mobile communications
HAL	hardware abstraction layer
HAV	Hardware Assisted Virtualization
HCL	hardware compatibility list
HDD	hard disk drive
HDMI	high definition media interface
HPFS	high performance file system
HTML	hypertext markup language
HTPC	Home Theater PC
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure sockets layer
I/O	input/output
ICMP	internet control message protocol
ICR	intelligent character recognition
IDE	integrated drive electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMAP	internet mail access protocol
IP	internet protocol
IPCONFIG	internet protocol configuration
IPP	internet printing protocol

IPSEC	internet protocol security
IR	infrared
IrDA	Infrared Data Association
IRQ	interrupt request
ISA	industry standard architecture
ISDN	integrated services digital network
ISO	Industry Standards Organization
ISP	internet service provider
JBOD	just a bunch of disks
Kb	kilobit
KB	Kilobyte or knowledge base
LAN	local area network
LBA	logical block addressing
LC	Lucent connector
LCD	liquid crystal display
LDAP	lightweight directory access protocol
LED	light emitting diode
Li-on	lithium-ion
LPD/LPR	line printer daemon / line printer remote
LPT	line printer terminal
LVD	low voltage differential
MAC	media access control / mandatory access control
MAPI	messaging application programming interface
MAU	media access unit or media attachment unit
Mb	megabit
MB	megabyte
MBR	master boot record
MBSA	Microsoft Baseline Security Analyzer
MFD	multi-function device
MHz	megahertz
MicroDIMM	micro dual inline memory module
MIDI	musical instrument digital interface
MIME	multipurpose internet mail extension
MIMO	Multiple Input Multiple Output
MMC	Microsoft management console
MMX	multimedia extensions
MP3	Moving Picture Experts Group Layer 3 Audio
MP4	Moving Picture Experts Group Layer 4
MPEG	Moving Picture Experts Group
MSCONFIG	Microsoft configuration

MSDS	material safety data sheet
MUI	multilingual user interface
NAC	network access control
NAS	network-attached storage
NAT	network address translation
NetBIOS	networked basic input/output system
NetBEUI	networked basic input/output system extended user interface
NFS	network file system
NIC	network interface card
NiCd	nickel cadmium
NiMH	nickel metal hydride
NLX	new low-profile extended
NNTP	network news transfer protocol
NTFS	new technology file system
NTLDR	new technology loader
NTP	Network Time Protocol
OCR	optical character recognition
OEM	original equipment manufacturer
OLED	Organic Light Emitting Diode
OS	operating system
PAN	personal area network
PATA	parallel advanced technology attachment
PC	personal computer
PCI	peripheral component interconnect
PCIe	peripheral component interconnect express
PCIX	peripheral component interconnect extended
PCL	printer control language
PCMCIA	Personal Computer Memory Card International Association
PDA	personal digital assistant
PGA	pin grid array
PGA2	pin grid array 2
PII	Personally Identifiable Information
PIN	personal identification number
PKI	public key infrastructure
PnP	plug and play
POP3	Post Office Protocol 3
PoS	Point of Sale
POST	power-on self test
POTS	plain old telephone service
PPP	point-to-point protocol

PPTP	point-to-point tunneling protocol
PRI	primary rate interface
PROM	programmable read-only memory
PS/2	personal system/2 connector
PSTN	public switched telephone network
PSU	power supply unit
PVC	permanent virtual circuit or polyvinyl chloride
PXE	preboot execution environment
QoS	quality of service
RAID	redundant array of independent (or inexpensive) disks
RAM	random access memory
RAS	remote access service
RDRAM	RAMBUS dynamic random access memory
RDP	Remote Desktop Protocol
RF	radio frequency
RFI	radio frequency interference
RGB	red green blue
RIMM	RAMBUS inline memory module
RIP	routing information protocol
RIS	remote installation service
RISC	reduced instruction set computer
RJ	registered jack
RJ-11	registered jack function 11
RJ-45	registered jack function 45
RMA	returned materials authorization
ROM	read only memory
RS-232 or RS-232C	recommended standard 232
RTC	real-time clock
SAN	storage area network
SAS	Serial Attached SCSI
SATA	serial advanced technology attachment
SC	subscription channel
SCP	secure copy protection
SCSI	small computer system interface
SCSI ID	small computer system interface identifier
SD card	secure digital card
SDRAM	synchronous dynamic random access memory
SEC	single edge connector
SFC	system file checker

SFF	Small Form Factor
SGRAM	synchronous graphics random access memory
SIMM	single inline memory module
SLI	scalable link interface
S.M.A.R.T.	self-monitoring, analysis, and reporting technology
SMB	server message block or small to midsize business
SMTP	simple mail transfer protocol
SNMP	simple network management protocol
SoDIMM	small outline dual inline memory module
SOHO	small office/home office
SP	service pack
SP1	service pack 1
SP2	service pack 2
SP3	service pack 3
SP4	service pack 4
SPDIF	Sony-Philips digital interface format
SPGA	staggered pin grid array
SRAM	static random access memory
SSH	secure shell
SSID	service set identifier
SSL	secure sockets layer
ST	straight tip
STP	shielded twisted pair
SVGA	super video graphics array
SXGA	super extended graphics array
TB	terabyte
TCP	transmission control protocol
TCP/IP	transmission control protocol/internet protocol
TDR	time domain reflectometer
TFTP	trivial file transfer protocol
TKIP	Temporal Key Integrity Protocol
TPM	trusted platform module
UAC	user account control
UART	universal asynchronous receiver transmitter
UDMA	ultra direct memory access
UDP	user datagram protocol
UNC	universal naming convention
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus

USMT	user state migration tool
UTP	unshielded twisted pair
UXGA	ultra extended graphics array
VESA	Video Electronics Standards Association
VFAT	virtual file allocation table
VGA	video graphics array
VM	Virtual Machine
VoIP	voice over internet protocol
VPN	virtual private network
VRAM	video random access memory
WAN	wide area network
WAP	wireless application protocol
WEP	wired equivalent privacy
WIFI	wireless fidelity
WINS	Windows Internet Name Service
WLAN	wireless local area network
WPA	wireless protected access
WUXGA	wide ultra extended graphics array
XGA	extended graphics array
ZIF	zero-insertion-force
ZIP	zigzag inline package

Appendix C: A Brief History of Personal Computers

Mechanical Computing Devices

Knowing a little about the history of computers can help you appreciate the current industry situation and prepare you for future developments. And, understanding how computers have evolved can help you appreciate how they are built and help you better understand why they work the way they do, which makes troubleshooting and repair that much easier.

The Abacus

The *abacus* is usually listed as the first mechanical computation device. Developed 2,000 or more years ago in India or the Far East, an abacus consists of columns of beads that can slide up and down on rods that are held together in a frame. The position of the beads represents a number. Skilled users could perform calculations more quickly than early electronic computers could.

Mathematical Advancements and Computing

The written number for zero appeared around 650 A.D. in India and made written calculations much easier. A Persian scholar wrote the first textbook on algebra in 830 A.D. During the 1100s, Europeans learned the written form of math used by the Arabs and wrote down multiplication tables to help merchants. Five hundred years later, John Napier, a Scotsman, carved a set of multiplication

tables on ivory sticks that could slide back and forth to indicate certain results. The use of logarithms on *Napier's Bones* in 1617 led to the development of the slide rule. Today's mature engineers can still remember using slide rules in their college days.

Calculating Machines

The Frenchman Blaise Pascal is usually given credit for the first calculating machine. In 1642, to help his father—a tax collector—with his work, Pascal invented a machine with eight metal dials that could be turned to add and subtract numbers. Leonardo da Vinci and Wilhelm Schickard, a German, designed calculating machines before Pascal, but Pascal receives the recognition because he produced 50 models of his *Pascaline machine,* not just a prototype or description. In 1673, Gottfried von Leibniz, a German mathematician, improved on Pascal's design to create a *Stepped Reckoner* that could do addition, subtraction, multiplication, and division. Only two prototypes were produced.

A Frenchman, Thomas de Colmar, created an Arithmometer in 1820 that was produced in large numbers over the ensuing 100 years. The Swedish inventor Willgodt T. Odhner improved on the Arithmometer, and his calculating mechanism was used by dozens of companies in the calculating machines they produced.

Punchcard Technologies

Punched cards first appeared in 1801. Joseph Marie Jacquard used the holes placed in the card to control the patterns woven into cloth by power looms. In 1832, Charles Babbage was working on a Difference Engine when he realized Jacquard's punched cards could be used in computations. The *Analytical Engine,* which is the machine Babbage designed but never manufactured, introduced the idea of using memory for storing results and the idea of printed output. His drawings described a general-purpose, fully program-controlled, automatic mechanical digital computer. Lady Ada Augusta Lovelace worked with Babbage on his machine. She became the first computer programmer when she wrote out a series of instructions for the Analytical Engine.

Note: Charles Babbage's Difference Engine No. 1 was the first successful automatic calculator. Although the 12,000 parts were never assembled into a finished engine, the parts that were completed functioned perfectly.

Punched cards were used in the United States census of 1890, and a data-processing machine created by Herman Hollerith tabulated the census results in only 2.5 years—much shorter than the predicted 10 years. Punched cards provided input, memory, and output on an unlimited scale for business calculating machines for the next 50 years. The company Hollerith founded to manufacture his card-operated data processors, which used electrical contacts to detect the pattern of holes in each card, eventually became IBM®.

Electronic Computers and the Military

With the beginning of World War II, electronic computers took on national importance. The accurate calculation of projectile trajectories became a life-and-death concern for the military. The

calculations needed to develop the atomic bomb also required more calculating power than was available before the war, and the calculations involved in trying to decode and break enemy codes saw researchers around the world start developing huge room-sized computers that could work on such problems more efficiently than a man with pencil and paper. Between 1939 and 1944, Howard H. Aiken developed the Harvard *Mark I*—also known as the IBM Automatic Sequence-Controlled Calculator (ASCC). The Mark I was made out of mechanical switches, electrical relays, rotating shafts, and clutches totaling 750,000 components weighing 5 tons. Programming instructions were fed to the Mark I on paper tape, and data was fed in on paper punched cards. Grace Hopper worked at Harvard on the Mark I, II, and III, and discovered the first real-life computer "bug" when she removed a moth that had flown into a mechanical relay, causing it to malfunction. Also, during the war, Konrad Zuse was working secretly on his Z3 computer in Germany. Because so little was known about the Z3 for so long, most people describe the Mark I as the first modern (but not electronic) digital computer.

Perhaps the most important and influential figure from this time was Alan Turing, an English mathematician who is now generally credited with being the father of computer science. Spending his time working in mathematics, logic, and cryptanalysis, Turing was heavily involved in Britain's codebreaking effort during World War II before he moved on to the University of Manchester. While at the University, he began work on the Manchester Mark I, one of the earliest computers. He is also credited with inventing the Turing Test, which has had profound implications in the development of Artificial Intelligence. The Turing Test was a low-tech test for the presence of Artificial Intelligence: if a person were to remotely converse by text with a human and a machine, and could not tell the difference between the two, then the machine would be said to pass the Turing Test.

Vacuum Tube Systems

The advent of vacuum tube technologies changed the face of electronic computing.

Vacuum Tubes and Digital Computing

Dr. John Vincent Atanasoff was an associate professor at Iowa State College when he designed an electronic digital computer that would use base two (binary) numbers. In 1939, with his assistant Clifford Berry, he built the world's first electronic digital computer using *vacuum tubes.* After a lecture, Dr. John W. Mauchly asked to see Atanasoff's computer and later used so many of Atanasoff's ideas in the ENIAC that it took a lawsuit to declare that Atanasoff was the first to use vacuum tubes in an electronic digital computer.

ENIAC to UNIVAC

Dr. Mauchly and J. Presper Eckert were at the University of Pennsylvania in 1942 when they built the *Electronic Numerical Integrator And Computer (ENIAC)* to aid the United States military during World War II. ENIAC used 18,000 vacuum tubes, had 500,000 hand-soldered connections, was 1,000 times faster than the Mark I, and had to be rewired to change its program. ENIAC was used from 1946 to 1955, and because of its reliability, it is commonly accepted as the first successful high-speed electronic digital computer. Eckert and Mauchly also designed the *Electronic Discrete*

Variable Automatic Computer (EDVAC), which contained 4,000 vacuum tubes and 10,000 crystal *diodes*. After their success with ENIAC, Eckert and Mauchly proposed to build a *Universal Automatic Computer (UNIVAC)* machine to help the Census Bureau handle all its data. After four years of delays and cost overruns, Remington Rand Inc. worked with the Eckert-Mauchly Computer Corporation to develop UNIVAC, the first commercially successful computer. The computer used magnetic tape to store data, a major change from IBM's punched cards, and introduced many other features that are common today. Starting in 1951, 46 UNIVAC I computers were made for the government and businesses, although some experts at the time thought that five computers would be enough to handle all the computational needs of the world.

John von Neumann

John von Neumann did not design the electronics in computers, but he is credited with the theoretical work that all modern computers are based on. Von Neumann recommended that a computer program should be able to stop under certain conditions and start again at another point. He also recommended storing both the data and instructions in memory so both could be changed as needed. He realized that physically rewiring a computer to change the program, or feeding in another paper tape to meet different conditions, was not practical for successful high-speed computing. The *Electronic Delay Storage Automatic Computer (EDSAC)* at Cambridge University, England, and Eckert and Mauchly's EDVAC were among the first to use von Neumann's ideas. Combining von Neumann's stored program concept with a 1,000-word main memory, magnetic tape for secondary memory, printer and typewriter output, and a 2.25 MHz clock rate, UNIVAC set the standard for computers in the 1950s.

Transistorized Systems and Other Technological Advances

In the 1950s, the progress of electronic computing was limited by technology. Vacuum tubes, which were used to control the flow of electricity in digital computer circuits, were large (several inches high), red-hot to touch, and unreliable. Transistor technologies were the next great technical step forward in the development of computing power.

Transistors

In the 1940s and early 1950s, Dr. William Shockley worked at Bell Telephone Laboratories as co-head of a solid-state research group that developed the *transistor.* Transistors performed the same function as vacuum tubes, but were the size of a pencil eraser, generated almost no heat, and were extremely reliable. The replacement of vacuum tubes with transistors opened up new possibilities.

Magnetic Core Memory

Another important innovation was *magnetic core memory,* which allowed information to be stored in the magnetic orientation of tiny magnetic rings strung together on fine wire. Using magnetic core memory, the huge mainframes increased their memory from 8,000 to 64,000 words. Combining the computational capability made available through transistors with expanded magnetic core memory gave computers so much power that they had to be used in new ways to justify the cost. Some mainframes used batch processing, where a series of programs and data was stored on magnetic

drums and fed to the computer one after the other so no computing time was wasted. Other computers used time sharing, where the computing power was shifted among several different programs running at the same time so no power was wasted waiting for an individual program's results to print or for more input to arrive.

Miniaturization and the Space Race

At this time, the United States and the former Soviet Union were involved in a race to see who would be first in space. The complex rockets demanded sophisticated computers to control them. The Soviet Union concentrated on designing bigger rockets to carry larger computers into space, while the United States worked on making smaller, more powerful computers that fit into the smaller rockets they had. The millions spent on research to miniaturize computer components used in the space race produced the technology needed for current computers.

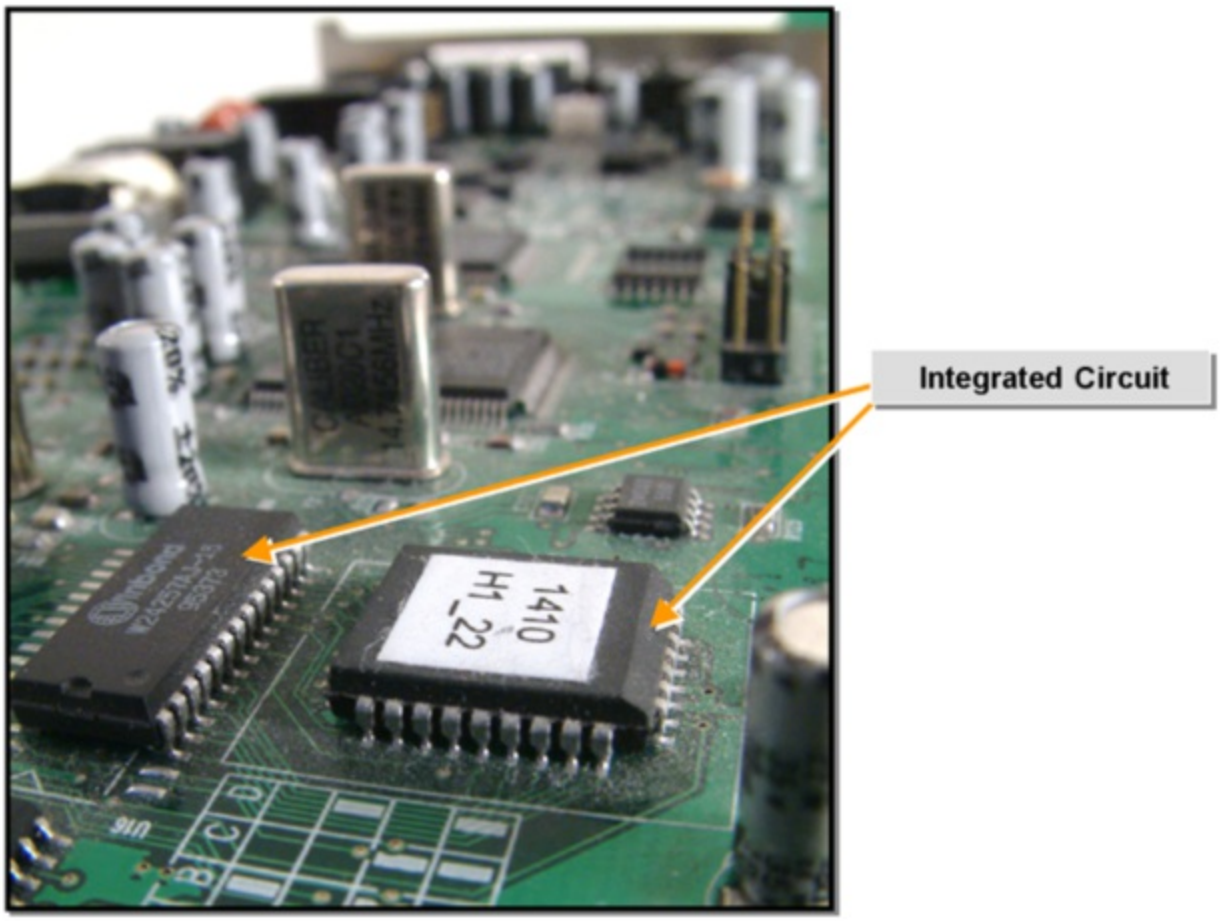
Integrated Circuit Technologies

The development of the integrated circuit paved the way for the computers we know today.

Integrated Circuits

Combining several transistors and the *resistors* needed to connect them on a single semiconductor chip in an *integrated circuit* was a tremendous technical advance. In 1958, Jack Kilby at Texas Instruments made several components on a single-piece semiconductor. By 1961, Fairchild and Texas Instruments were mass-producing integrated circuits on a single chip. In 1967, Fairchild introduced the Micromosaic, which contained a few hundred transistors. The transistors could be connected into specific circuits for an application using computer-aided design. The Micromosaic was an Application-Specific Integrated Circuit (ASIC).

Note: Now usually called just a chip, the first integrated circuit was fabricated in 1958 by Texas Instruments inventor Jack Kilby.



Early RAM and Processor Circuits

In 1970, Fairchild introduced the first 256-bit static *RAM chip,* while Intel® announced the first 1,024-bit dynamic RAM. Computers that could make use of this memory were still monsters to maintain. Handheld calculators, on the other hand, appealed to everyone from scientists to school kids. Marcian "Ted" Hoff at Intel designed a general-purpose integrated circuit that could be used in calculators, as well as other devices. Using ideas from this circuit, Intel introduced, in 1972, the *8008,* which contained approximately 3,300 transistors and was the first *microprocessor* to be supported by a high-level language compiler called PL/M.

General-Purpose Microprocessors

A major breakthrough occurred in 1974 when Intel presented the 8080, the first general-purpose microprocessor. The 8080 microprocessor had a single chip that contained an entire programmable computing device on it. The 8080 was an 8-bit device that contained around 4,500 transistors and could perform 200,000 operations per second. Other companies besides Intel designed and produced microprocessors in the mid-1970s, including Motorola (6800), Rockwell (6502), and Zilog (Z80). As more chips appeared and the prices dropped, personal desktop computers became a possibility.

Personal Computers

These developments led to the personal computer that is ubiquitous in homes and businesses today.

The First PCs

About a dozen computers claim to be the first *Personal Computer (PC)*. Credit for the first popular personal computer often goes to Ed Roberts, whose company, MITS, designed a computer called the Altair 8800 and marketed a kit for about $400 in 1974. The Altair 8800 used Intel's 8080 microprocessor, contained 256 bytes of RAM, and was programmed by means of a panel of toggle switches. In 1975, Bill Gates and Paul Allen founded Microsoft® and wrote a BASIC interpreter for the Altair. More than 2,000 systems were sold in 1975.

In 1975, MOS Technology announced its 6502-based KIM-1 desktop computer, and Sphere Corporation introduced its Sphere 1 kit. Both kits were strictly for computer fanatics.

Early General-Purpose PCs

In 1976, Steve Wozniak and Steve Jobs formed Apple® Computer Inc., and began creating their first commercial product, the Apple I. Unique for the time, the Apple I was a relatively inexpensive hobbyist computer that required users to provide their own case, monitor, keyboard and power supply. The Apple I was later modified to create the Apple II (with a 6502 microprocessor). In 1977, the Apple II cost $1,300, came with 16 KB of ROM, 4 KB of RAM, a keyboard, and color output. The Apple II is usually listed as the first personal computer that was available for the general public. The Commodore PET (6502) and Radio Shack's TRS-80 (Z80) were also popular. In 1979, VisiCalc, a spreadsheet program for the Apple II, made desktop computers attractive to businesses. As more businesses bought Apples, demand appeared for word-processing applications, and the software development industry took off. In 1981, IBM joined the party with its first PC. Dozens of other models and companies followed IBM's lead, but in 1984, Apple broke from the pack and produced the Macintosh® computer with a mouse and graphical user interface that opened the computer world

to artists and publishers. Of all the computers designed during this period, only the IBM PC and Apple Macintosh have withstood the test of time.

Today's PCs

Today there are several types of PCs, including desktop, minitower, laptop, netbook, tablet PC, and handheld PDA. Most mobile devices have many of the functions of a small computer and the distinction between computer and communications device is blurring.

The Development of the Graphical User Interface

With the near-ubiquity of personal and portable computers today, it is difficult to imagine a time when computers were large, expensive, took several days to process a request and, most importantly, could only understand instructions via a series of card punches. However, this accurately describes many computers well into the early 1970s. Therefore, alongside the development of the microprocessor, one of the most important technological developments encouraging the wide adoption of easy-to-use personal computers has been the development of the graphical user interface (GUI).

Douglas Engelbart, a researcher at the Stanford Research Institute (SRI), is widely credited with developing the first GUI. Engelbart's research borrowed heavily from ideas spelled out by Vannevar Bush's 1945 essay titled "As We May Think." In this essay, Bush proposed a machine called a memex, which was a hypothetical way of navigating through large amounts of information using hypertext. The memex was based on how adults actually learn, store, and process information, and had increased relevance in an age where information was rapidly changing. While the memex was never created, Engelbart borrowed heavily from Bush's ideas when it came time to work on his own hypertext-based visual computer called the On-Line System, or NLS. The NLS debuted in 1968, and featured the first uses of a GUI, hypertext, a mouse, windows for organizing and displaying information, the use of a computer to deliver a presentation, and many other now-common computer features.

Note: Vannevar Bush's 1945 essay "As We May Think" can be read online at **www.theatlantic.com/doc/194507/bush**.

Note: A full-length video of Doug Engelbart's demo of the NLS can be found online at **www.1968demo.org/**.

After the SRI's introduction of the NLS, work continued on graphical user interface design at Xerox PARC (Palo Alto Research Center). Xerox PARC created what many now consider the first personal computer that used a GUI, along with the now-familiar desktop metaphor. Dubbed the Xerox Alto, it was the first small-scale computer where a graphical tool could be used to create, delete, and manage local files—the Alto was *not* merely a terminal.

Apple founder Steve Jobs visited Xerox PARC, and during his visit became very interested in the mouse. The Alto was not available commercially for home use, but Apple was targeting a larger

market. He incorporated what he liked about the Alto into Apple's design, and so the first two GUI computers from Apple—the Lisa and the MacIntosh—featured both a GUI and a mouse. Apple's GUIs also continued the Alto's use of the desktop metaphor, with icons of documents and folders representing files and directories. This proved to be an enormously popular way to use a personal computer. Shortly after Apple debuted their GUI, Microsoft released their first operating system that had a graphical interface. Windows 1.0 was a GUI that ran on top of the existing MS-DOS operating system, which was purely text-based up until that point.

Windows greatly changed the look and feel of their GUI with the release of Windows® 95 (the first 32-bit version of Windows), and subsequent Windows operating systems have stayed fairly true to that design: this was the first use in Windows of the Start menu and taskbar, which have been mainstays for more than a decade. Most operating system GUIs since then have shared this basic layout, though the complexity of the graphics may have evolved.

Graphical interface design today has gotten both grander and smaller. With the exploding popularity of handheld multimedia devices, GUIs are no longer limited just to PCs. Thanks to cell phones and smartphones, MP3 players, mobile Internet devices, ebook readers, and more, interfaces have the added challenge of needing to operate on very small screens, drawing far less power, and using weaker processors. On top of this, interface development has had to straddle the line between graphical appeal (such as with 3D desktops) and usability (where the drive for a more user-friendly interface outweighs any flashier graphical features).

Computing Today and Tomorrow

Today, in the early 21st century, computers and computing have become ubiquitous in the daily lives of almost everyone in the developed world. Computers are present not only as home and office productivity tools, but also as enhancements to everything from home appliances to SUVs. There is more computing power in the average consumer's automobile today than there was on board the Apollo spacecraft that took human beings to the moon and back in the 1960s and 1970s.

The Internet is no less influential than the PC in today's interconnected world. Since physicist Tim Berners-Lee of the CERN laboratory invented the basic technologies of the World Wide Web and posted the first website in 1991, the growth of the Internet has exploded to the point where virtually all computers on the planet are interconnected. Ordinary users can now communicate sophisticated information with each other instantaneously around the globe. The ongoing vision of "Web 2.0" may soon create a global society in which all types of information and all means of communication will be created and maintained cooperatively by ordinary individuals throughout the world. There is even a drive toward turning computers into little more than bootable machines with web browsers on them. In this system of "cloud computing," all computing power is provided through remote computers that function, essentially, as application servers. Microsoft's Office 365™ is a prime example of cloud computing, and all reports indicate that cloud computing is here to stay.

The ubiquity of computing power and the omnipresence of the Internet: these two factors have changed our world to an unimaginable extent in an extraordinarily short period of time. Society as a whole can look forward eagerly to the equally unimaginable and extraordinary changes technology

will bring us in the years and decades just ahead.

Lesson Labs

Lesson labs are provided for certain lessons as additional learning resources for this course. Lesson labs are developed for selected lessons within a course in cases when they seem most instructionally useful as well as technically feasible. In general, labs are supplemental, optional unguided practice and may or may not be performed as part of the classroom activities. Your instructor will consider setup requirements, classroom timing, and instructional needs to determine which labs are appropriate for you to perform, and at what point during the class. If you do not perform the labs in class, your instructor can tell you if you can perform them independently as self-study, and if there are any special setup requirements.

LAB 1-1: Identifying Hardware Components

Activity Time: 10 minutes

Scenario

In this lab, you will identify the hardware components for several PCs.

1. Examine as many of the PCs that are in your environment as you can.
2. For each system:
    a. Locate the primary components, and determine what types of input devices, output devices, and external devices are present.
    b. Determine the type and form factor. For instance, is the system a desktop PC, a tower PC, a laptop, or some other type of system?
    c. Identify the ports available on the computer. See if you can tell which ports are built-in and which are provided by adapter cards.
    d. Try to determine what types of internal storage devices the system provides.

LAB 2-1: Identifying Operational Procedures

Activity Time: 10 minutes

Scenario

In this lab, you will identify operational procedures and best practices for PC technicians.

1. **List the items that you would want to have in your hardware toolkit.**

   A: Answers will vary, but should include at least a large and small flat-head screwdriver, a large and small Phillips screwdriver, a pen or pencil, a flashlight, a container for screws, and a nut driver.

2. **Select the items that can pose an electrical hazard.**

   _x_ Chassis
   _x_ Monitor
   __ Printer
   _x_ Power supply
   __ Battery
   _x_ Capacitor

3. **Consider this scenario: A novice technician arrives at a user's workspace to troubleshoot a sound card. The user assures the technician that the power to the PC is off. As the technician begins working, he finds that the anti-static wrist strap gets in the way, so he removes it. Once the PC cover is off, the technician pulls the sound card out of the expansion slot and places it on a nearby metal filing cabinet, replacing it with a network card that he knows works properly. Finding that the network card does not work when installed in that expansion slot, the technician determines that there is a resource conflict, corrects the conflict, and replaces the network card with the user's original sound card. After testing the sound card, the technician and user agree that the problem is resolved. As the technician is repacking his toolkit, the user mentions a funny ozone smell coming from her laser printer. The technician assures the user that an occasional whiff of ozone is normal, and ends the service call. What would you do differently?**

   A: Responses should include the following safe practices: Never assume anything; verify for yourself that the power is off and power cables are unplugged before starting the troubleshooting process. No matter how uncomfortable it seems, wear the anti-static wrist strap and connect it to ground unless you are working on power supplies or monitors. Always store electronic parts that you intend to reuse in anti-static bags or on a dissipative mat. Check the area surrounding the laser printer to ensure that the

printer is properly ventilated; if the airflow seems adequate, the ozone filter in the printer might need to be replaced.

4. **What are some examples of active listening techniques?**

_x_ Paraphrasing the user's comments.
__ Nodding your head, and maintaining eye contact.
__ Avoiding interrupting the user by writing down your questions.
_x_ Empathizing with the user.
_x_ Using open-ended questions to gather information about the problem that the user is experiencing.

LAB 3-1: Installing and Configuring Peripheral Components

Activity Time: 30 minutes

Before You Begin

To complete this activity, you will need the following hardware components. If you do not have these available, you can remove and reinstall the existing hardware:

- An external monitor.
- A keyboard and mouse or other pointing device.
- An expansion card.
- A multimedia device.

Scenario

You have been asked to assist a user whose computer needs refurbishing. You have several new peripheral components to install, configure, and verify for the user.

Note: You can find a suggested solution for this activity in the Solution\Installing and Configuring Peripheral Components.txt file in the data file location.

1. Install and configure the monitor.
2. Install and configure the input devices.
3. Install and configure the multimedia device.

LAB 4-1: Managing System Components

Activity Time: 15 minutes

Before You Begin

To complete this lab, you will need the following hardware components. If you do not have these available, you can remove and reinstall the existing hardware:

- An optical drive that is compatible with your system.
- Optionally, rails to allow smaller drives to fit into larger drive bays.

Scenario

You have been assigned the task of repairing a computer for a client. The computer has an optical drive that needs to be replaced, and a PATA optical drive has been allocated for the task.

1. Remove the old optical drive from the computer.
2. Install the new optical drive in the computer.

LAB 6-1: Selecting and Using Networking Technologies

Activity Time: 45 minutes

Before You Begin

You will need two Windows 7 computers. Both computers must be connected to the Internet. You will also need a headset with a microphone, or a microphone and speakers, attached to each computer. If you have a partner, you can work with a partner to complete the hands-on portion of the lab. If you have existing Skype account information, you can use that in lieu of creating a new account for each Skype system.

Scenario

You are a support technician for My Footprint Sports. My Footprint Sports is opening a new retail store in the Midwest, and you have been assigned to support the installation of the new site. Your first duty is to work on a team to help identify the various network technologies the new store will require to enable its employees to communicate electronically both with the network servers that control operations from the head office in Greene City, as well as with other My Footprint Sports employees, preferred customers, colleagues, and suppliers throughout the world. Store managers and assistant managers have been issued wireless laptops that will need to be integrated into the store's network structure.

1. **List the various networking technologies you would recommend for the My Footprint Sports retail outlet, and explain how each technology would support the employees' connectivity needs. Are there any network components that you would not employ? Are there any optional components? What are the pros and cons of implementing each one? You might wish to sketch a possible network design for this store to show the various connectivity components.**

   A: The new store will require a local Ethernet LAN installation, probably using a twisted-pair media with the appropriate cables and connectors. If the store is configured to use the client-server resources available at headquarters, rather than in a workgroup, you do not have to worry about configuring multiple user accounts on the individual computers. Because the store employees need to communicate globally, they will need Internet access. It is unlikely that My Footprint Sports has a direct Internet connection, so the company will need to contract with a business-oriented ISP. Because of their communications needs, employees will need a high-speed, continuous high-bandwidth Internet connection. Selecting the particular connection technology will be a matter of negotiating the best combination of price and service with the available local ISPs. For Internet access, the local computers will need to run the TCP/IP protocol. There is no indication from the scenario that the store will need to run any legacy network protocols other than TCP/IP. The ISP will probably provide addressing

and name resolution services. Employees will need email access. Because they are part of a larger organization, My Footprint Sports, rather than the ISP, will probably provide the email infrastructure and email addresses within the **www.myfootprintsports.local domain.** My Footprint Sports probably has email servers already implemented to provide SMTP services as well as POP3 and/or IMAP4 client protocols, depending upon the email client software in use at the company. The store will need to install Wi-Fi-capable WAPs to support the integration of the wireless laptop users with the wired Ethernet in the rest of the store, as well as for other workers with laptops. Other types of wireless support might or might not be needed depending upon the requirements of individual users; for example, there might be some staff who use Bluetooth to synchronize mobile-device data with their personal computers, and there might be wireless infrared peripheral devices in use, such as wireless mice. Staff do need to communicate globally. If they need to make a lot of international phone calls, the team might consider implementing VoIP connections to make voice phone calls over the existing Internet connections and save the incremental phone charges. Any other specialized networking tools, such as FTP client software, will depend upon the corporation's and individual users' communications needs.

2. The decision has been made by management to investigate VoIP communications to help reduce the cost of long-distance telephone calls. Management has also asked for some ideas on accessing and troubleshooting remote servers. You know a little about Skype for Internet-based voice communication and Telnet for remote communication, but you want to test the features of Skype and Telnet before suggesting them to management as potential solutions. Download the Skype software from the **www.skype.com** website.
3. Follow the on-screen installation instructions, and install the software on both systems.
4. Either create a new Skype account on each system by entering a user name and password, or sign in to an existing Skype account on each system.
5. Check your sound equipment and make a test call.
6. Add the Skype account to the contact list of the other PC.
7. Initiate a Skype session between the two computers.
8. Disconnect from the call, sign out of Skype, and close the Skype window.
9. Enable Telnet.
10. In your web browser, open the www.telnet.org website and click the link for **places to telnet** to obtain addresses of remote hosts that maintain open Telnet connections. Some of the addresses are followed by any public login information you may need.
11. In a command prompt, initiate a Telnet session with a remote host. If you are unsuccessful in connecting, try **www.scn.org** or **www.torfree.net.**
12. After you connect to the remote host, log in (using the suggested login information from the **places to telnet** link) and investigate the commands and features offered by the remote host.
13. Disconnect the Telnet connection, and close all open windows.

Glossary

8008

Introduced by Intel in 1972, the 8008 was the first microprocessor to be supported by a high-level language compiler.

802.11

A family of specifications for wireless LAN communication.

802.11a

A fast, secure, but relatively expensive protocol for wireless communication. The 802.11a protocol supports speeds up to 54 Mbps in the 5 GHz frequency.

802.11b

Also called Wi-Fi, short for "wireless fidelity," 802.11b is probably the most common and certainly the least expensive wireless network protocol used to transfer data among computers with wireless network cards or between a wireless computer or device and a wired LAN. The 802.11b protocol provides for an 11 Mbps transfer rate in the 2.4 GHz frequency.

802.11e

A wireless LAN communication standard for home and business implementations.

802.11g

A specification for wireless data throughput at the rate of up to 54 Mbps in the 2.4 GHz band that is a potential replacement for 802.11b.

802.11n

A recent specification for wireless data throughput at a rate up to 600 Mbps in the 2.4 GHz or 5 GHz range. Released in 2009.

abacus

An early calculating instrument that uses sliding beads in columns that are divided in two by a center bar.

accelerometer

Mobile technology that can determine the orientation of a device with a sensor that measures the acceleration of the device direction.

Action Center

A utility unique to the Windows 7 Control Panel in which notifications can be enabled or disabled, and alerts are consolidated into a single location.

activity light

An indicator on a network adapter that flickers when packets are received or sent.

administrative shares

Hidden shares created by default on every Windows system. If administrative shares are deleted, by default, the system re-creates them when it restarts.

adware

Unwanted software loaded onto a system for the purposes of presenting commercial advertisements to the user.

Aero

A color scheme available in Windows Vista and Windows 7 that provides a visually rich experience, with a glossy and transparent interface and dynamic visual effects.

AES

(Advanced Encryption Standard) A symmetric 128-, 192-, or 256-bit block cipher based on the Rijndael algorithm developed by Belgian cryptographers Joan Daemen and Vincent Rijmen and adopted by the U.S. government as its encryption standard to replace DES.

AGP

(Accelerated Graphics Port) A bus architecture based on PCI and designed specifically to speed up the rendering of 3D graphics.

AIO MFD

(all-in-one multi-function device) A small sized MFD for home users with basic printing, scanning, and copying functions.

allocation unit

Same as cluster.

analog signal

A signal that oscillates over time between minimum and maximum values and can take on any value between those limits.

analog transmission

The transfer of information in the form of a continuous wave.

Analytical Engine

Charles Babbage's vision of a mechanical calculator that would follow programmed instructions to perform any mathematical operations. The engine could store results for use later, and look up values

in tables and call on standard subroutines.

Android

An operating system for mobile devices such as smartphones.

anti-spyware software

Software that is specifically designed to protect systems against spyware attacks.

antivirus software

An application that scans files for executable code that matches patterns known to be common to viruses, and monitors systems for activity associated with viruses.

AP

(access point) A device or software that facilitates communication and provides enhanced security to wireless devices.

APIPA

(Automatic Private IP Addressing) A feature of Windows that enables a DHCP client computer to configure itself automatically with a random IP address in the range of 169.254.0.1 to 169.254.255.254 if there is no DHCP server available.

ASR

(Automated System Recovery) A Windows XP troubleshooting tool that enables you to back up data and Windows installation source files for rebuilding a failed system.

ATA

(Advanced Technology Attachment) The official ANSI term for IDE drives.

ATX

An older motherboard that was introduced by Intel in 1995 to provide better I/O support, lower cost, easier use, and better processor support than even earlier form factors.

audio/video editing workstation

A powerful computer setup that supports the editing of audio and video recordings.

AUP

(acceptable use policy) A policy that includes the practices and guidelines that should be followed by employees when using and accessing company resources and computer equipment.

auto negotiation

Negotiates a speed that is compatible with the network router or switch.

backlight

The typical form of illumination used in a full-sized LCD display.

badges

Also called security cards, that can be used to swipe through an identification system or can be configured as a proximity card and activated automatically when the card is within a specified distance from the system

baseband

A transmission scheme where a single signal sends data using the entire bandwidth of the transmission media. Compare with broadband.

battery backup

See UPS.

biconic

A screw-on type connector with a tapered sleeve that is fixed against guided rings and screws onto the threaded sleeve to secure the connection.

biometrics

Authentication schemes based on individuals' physical characteristics.

BIOS

(Basic Input/Output System) A set of instructions that is stored in ROM and that is used to start the most basic services of a computer system.

BIOS memory

Special memory that keeps track of its data even when the power is turned off, and is stored in EEPROMs.

BitLocker

A security feature in Windows 7 and Windows Server 2008 that provides full disk encryption protection for your operating system as well as all the data stored on the operating system volume.

blackout

A complete loss of electrical power.

bluejacking

A method used by attackers to send out unwanted Bluetooth signals from PDAs, mobile phones, and laptops to other Bluetooth-enabled devices.

bluesnarfing

A process in which attackers gain access to unauthorized information on a wireless device using a Bluetooth connection.

Bluetooth

A wireless radio technology that facilitates short-range (usually less than 30 feet) wireless communication between devices such as personal computers, laptop, mobile phones, wireless headsets, and gaming consoles, thus creating a wireless personal area network.

BNC

(Bayonet Neill-Concelman) A twist lock connector that is used with coaxial cable to carry radio frequencies to and from devices.

bootrec

A command line tool used via the Command Prompt in the Windows Recovery Environment In Windows Vista and Windows 7 only to troubleshoot or repair startup issues.

bridge

A network device that divides a logical bus network into subnets.

brightness

The amount of light emitted from a display device, as measured in lumens.

broadband communications

A category of network transmission technologies that provide high throughput by splitting communications pathways into multiple channels transmitted simultaneously over the network media.

brownout

A temporary power reduction that is used by electrical power companies to deal with high power demands.

BSOD

The blue screen of death error that is severe enough to stop all processes and shut the system down without warning.

bus

In a computer system, a group of wires that connect components. They provide a pathway for data transfer.

bus topology

A network topology where all nodes receive transmitted data at the same time, no matter how the

physical wiring is configured.

cable

Transmissions that use a cable television connection and a specialized interface device known as a cable modem to provide high-speed Internet access to homes and small businesses.

cable tester

An electrical instrument that verifies if a signal is present on a cable. Also called a media tester.

cache memory

A type of memory that services the CPU. Level 1 (L1) cache is built into the CPU chip. Level 2 cache (L2) feeds the L1 cache. L2 can be built into the CPU chip, reside on a separate chip, or be a separate bank of chips on the system board. If L2 is built into the CPU, then level 3 cache (L3) can be present on the system board.

CAN

(campus area network) A network that covers an area equivalent to an academic campus or business park.

carputers

Wireless computing devices that are specifically designed for cars. Many devices include features such as GPS, media players, USB, and Bluetooth communications.

CCFL

(cold cathode fluorescent lamp) A light source that uses electrodes and mercury vapor to create ultraviolet light.

cd

A command line tool used to view the drive letter and folder for your current location, and to change to another directory or folder.

CDFS

(Compact Disc File System) A file system standard for optical disc media that is supported by multiple operating system types.

cellular

Uses radio signals to transmit network data over the cellular telephone system.

chain of custody

The record of evidence history from collection, to presentation in court, to disposal.

chipset

The set of chips on the system board that support the CPU and other basic functions.

chkdsk

A command line tool used to identify hard drive errors and correct the error, if possible.

Class A addresses

An IP subnetting scheme that provides 16,777,214 nodes per network.

Class B addresses

An IP subnetting scheme that provides 65,534 nodes per network.

Class C addresses

An IP subnetting scheme that provides 254 nodes per network.

client

A computer that makes use of the services and resources of other computers.

client-side virtualization

Takes place at the endpoints and separates the elements of a user's logical desktop environment—the applications, operating system, programs, etc.—and divides them from each other and from the physical hardware or a physical machine.

client/server network

A network in which some computers act as servers to provide special services for other client computers.

closed source

Refers to any application code, programming code, or operating system code that is not published or shared with the community.

cluster

A group of sectors that is the smallest unit of storage allotted on a given drive.

CMOS

(Complementary Metal-Oxide-Semiconductor) An old style of static memory that was used to store information about the computer setup that the system BIOS refers to each time the computer is started.

coax

Pronounced "CO-ax." A common abbreviation for coaxial cable.

coaxial cable

A type of cable that features a central conductor surrounded by braided or foil shielding. A dialectric insulator separates the conductor and shield and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

Component Services

An administrative tool that is used to deploy component applications and configure the behaviors of components and applications on the system.

component/RGB

A type of analog video information that is transmitted or stored as two or more separate signals.

composite video

The format of an analog (picture only) signal before it is combined with a sound signal and modulated onto a radio frequency (RF) carrier.

computer case

The enclosure that holds all of the components of your computer.

computer connection

A hardware component that enables the computer to communicate with internal or external devices.

computer forensics

Collecting and analyzing data from storage devices, computer systems, networks, and wireless communications and presenting this information as a form of evidence in a court of law.

computer image

A replica of the reference computer's hard disk and contains the operating system software used in the imaging process.

Computer Management

The primary administrative tool used to manage and configure the system. It consolidates several administrative utilities into a single console to provide easy access to the most common system tools.

controller

See disk controller.

cooling system

A system unit component that prevents damage to computer parts by dissipating the heat generated inside a computer chassis.

corona

An assembly within a laser printer that contains a wire (the corona wire), which is responsible for charging the paper.

CPU

(central processing unit) The main chip on the system board, the CPU performs software instructions and mathematical and logical calculations. Also referred to as the microprocessor or processor.

CRT display

(cathode ray tube) A display device that uses three electron beams, one for each primary color (red, blue, and green), within a vacuum tube to create images on a fluorescent screen.

data backup

A system-maintenance task that enables you to store copies of critical files and folders on another medium for safekeeping.

data restoration

A system recovery task that enables you to access the backed-up data.

Data Sources

An administrative tool that uses Open Database Connectivity (ODBC) to move data between different types of databases on the system.

data synchronization

The process of automatically merging and updating common data that is stored on multiple devices.

data wiping

A method used to remove any sensitive data from a mobile device and permanently delete it.

daughter board

Any circuit board that plugs into another circuit board.

DB-15

See VGA.

dead pixels

Pixels that do not display light as expected and will show up as small black dots.

Defender

The anti-spyware software that is included with Windows XP, Vista, and 7 installations.

definition

A code pattern that identifies a virus. Also called a signature.

del

A command line tool used to delete a file.

device driver

Software that enables the operating system and a peripheral device to communicate with each other. Often referred to as driver software or driver.

Device Manager

An administrative tool that is used to manage and configure system devices in a hardware profile.

DHCP

(Dynamic Host Configuration Protocol) A network service that provides automatic assignment of IP addresses and other TCP/IP configuration information on network systems that are configured as DHCP clients.

dial-ups

Local-loop phone connections that use modems and standard telephone technology.

digital signal

An electrical signal that holds only two values: ones and zeros.

digital transmission

The transfer of information in a signal that is comprised only of ones and zeroes.

DIMM

(Dual In-line Memory Modules) A RAM form factor that is found in most systems and that has a 64-bit data path.

diode

An electronic component that acts like a one-way valve. Diodes are often used to change Alternating Current (AC) to Direct Current (DC), as temperature or light sensors, and as light emitters.

DIP switches

A switch that is connected to the motherboard that allows you to configure the electric circuits located on the board.

direct thermal printer

A thermal printer that uses heated pins to form images directly onto specially coated thermal paper.

directory

A component in a file system hierarchy that provides a container to organize files and other directories (folders). Also called a folder.

directory service

On a network, a centralized database that includes objects such as servers, clients, computers, user names, and passwords, and provides centralized administration and authentication.

discovery mode

A device mode that will transmit a friendly signal to another device in close proximity.

disk controller

Circuitry that manages the transfer of data to and from a disk drive, whether it is a floppy disk drive, a hard disk drive, or an optical disk drive. The disk controller provides the communication path between the CPU and the disk drive.

disk partition

An isolated section of a disk that functions like a separate physical drive.

diskpart

A command line tool used to create, delete, or generally manage any hard drive partitions on the system.

display device

A personal computer component that enables users to view the text and graphical data output from a computer.

DisplayPort

A digital display standard that aims to replace DVI and VGA standards.

dissipative material

A conductor, but with high resistance that loses its electrical charge slowly.

DMZ

(demilitarized zone) A small section of a private network that is located between two firewalls and made available for public access.

DNS

(Domain Name System) The primary name resolution service on the network that maps computer names to their associated IP addresses.

docking station

Desktop devices that connect portable computers to standard desktop peripherals without the need to

connect and disconnect the peripherals themselves when the user switches from stationary to mobile use.

domain

A Microsoft network model that an administrator implements by grouping computers together for the purpose of sharing a centralized user account database. Sharing this user account database enables users to use these accounts to log on at any computer in the domain.

domain controller

A server that stores the user account database for the domain and is responsible for authenticating users when they log on to the domain.

dongle

A short adapter cable used to connect a PC Card to a full-sized connector, or a device that attaches to a computer port to control access to a particular application.

dot-matrix printer

An impact printer that forms images out of dots on paper by using a set of pins to strike an inked ribbon.

drive rails

Metal strips that can be screwed onto an internal drive before installation.

DSL

A broadband technology that transmits digital signals over existing phone lines.

dump file

The file that stores the contents of a memory dump.

duplex scanning

A feature that scans both sides of a document automatically.

duplexing

Disk mirroring in which the two drives in the mirror each have a dedicated disk controller.

duplexing

The process that enables automatic printing on both sides of printing media, such as paper and envelopes.

duplexing assembly

A component that moves printing media through a printer twice to allow for double-sided printing.

DVI

(Digital Video Interface) A cable that keeps data in digital form from the computer to the monitor.

dye sublimation printer

Same as thermal dye transfer printer.

dynamic addressing

A method used to assign addresses using the DHCP service.

EAS

(Exchange ActiveSync) Microsoft's synchronization protocol that enables mobile devices to connect to an Exchange Server to access mail, calendar and contacts.

Easy Transfer

A built-in data migration utility in Windows Vista and Windows 7 that helps transfer files, data, and settings from one personal computer to another.

ECC

(Error Correction Code) An error correction method that uses several bits for error-checking.

EDSAC

(Electronic Delay Storage Automatic Computer) A well-engineered machine built by Maurice Wilkes and colleagues at the University of Cambridge Mathematics Lab in 1949 that was a productive tool for mathematicians.

EDVAC

(Electronic Discrete Variable Automatic Computer) The first computer to use stored programs.

EEPROM

(electronically erasable programmable read-only memory) A ROM chip that can be reprogrammed by using software from the BIOS or chip manufacturer through the flashing process.

EIA

(Electronic Industries Alliance) A standards and trades organization that developed industry standards for technologies such as network cabling. The EIA ceased operations in February 2011.

electrical interference

A general term for unwanted signals on the network media that can interfere with network transmissions.

electrical noise

The same as electrical interference.

EMI

(electromagnetic interference) The degradation of signal that occurs when a magnetic field around one electrical circuit interferes with the signal being carried on an adjacent circuit.

emulator

The software installed that allows the computer to virtually run another operating system, or another instance of the same operating system.

encryption

The process of converting data into a form that is not easily recognized or understood by unauthorized entities.

ENIAC

(Electronic Numerical Integrator And Computer) Developed for the U.S. Army by J. Presper Eckert and John Mauchly at the University of Pennsylvania in Philadelphia. ENIAC was programmed by plugging in cords and setting thousands of switches to direct how 18,000 vacuum tubes would perform 5,000 calculations per second.

EP drum

(Electrostatic Photographic drum) The component in a laser printer that carries the electrical charge to attract toner and then to transfer the toner to the paper.

ERD

(emergency repair disk) A Windows XP troubleshooting tool that stores the contents of the \Windows\Repair folder.

ESD

(electrostatic discharge) The phenomenon that occurs when electrons rush from one body with a static electrical charge to another with an unequal charge, following the path of least resistance.

Ethernet

A family of networking technologies that provide connectivity by using Ethernet network adapters, contention-based media access, and twisted pair, coax, or fiber media.

Event Viewer

An administrative tool that is used to view the contents of event logs, which contain information about significant events that occur on your computer.

evil twin

A rogue wireless access point that appears to be a legitimate one offered on the premises, but actually

has been set up to eavesdrop on wireless communications among Internet surfers.

expansion card

A printed circuit board that is installed in a slot on a system board to provide special functions for customizing or extending a computer's capabilities. Also referred to as adapter card, I/O card, add-in, add-on, or board.

ExpressCard

A mobile expansion card designed by the PCMCIA to replace traditional PC Cards to provide PCI Express and USB 2.0 connectivity.

external device

Devices that provide alternative input or output methods or additional storage for personal computers.

external enclosure

A plastic barrier that protects the inner workings of a hard drive.

F-connector

A coaxial cable connector used to connect TV and FM antennas.

factory recovery partition

A hidden partition on the hard disk containing the files and settings needed to do a fresh install of the operating system and pre-installed applications in order to restore the computer to factory settings.

FC

(Face Contact) Connectors that use a heavy duty ferrule in the center for more mechanical stability than SMA or ST connectors.

FC-AL

(Fibre Channel-Arbitrated Loop) A Fibre Channel implementation that can connect up to 127 nodes without using a switch. All devices share the bandwidth, and only two can communicate with each other at the same time, with each node repeating the data to its adjacent node.

FDD

(floppy disk drive) A personal computer storage device that reads data from and writes data to removable disks made of flexible Mylar plastic covered with a magnetic coating, and enclosed in a stiff, protective, plastic case. It is a legacy technology.

FDDI

(Fiber Distributed Data Interface) A push/pull type, two-channel snap-fit connector used for multimode fiber optic cable. Also called a MIC (Media Interface Connector).

fdisk

A command line tool used to partition or re-partition a hard drive.

fiber

A method used to connect devices the Internet using fiber optic cable.

fiber optic cable

A type of cable in which one or more glass or plastic strands, plus additional fiber strands or wraps, are surrounded by a protective outer jacket. Light pulses carry the signal through fiber optic cable.

file attribute

A characteristic that can be associated with a file or folder that provides the operating system with important information about the file or folder and how it is intended to be used by system users.

file recovery software

Software that can recover deleted files from your computer system.

file system

An inherent organizational structure that is used to organize and store data and information in a logical manner on a system's storage device.

Files and Settings Transfer Wizard

A system tool that is available in Windows XP and earlier versions of Windows that transfers files and settings from an old computer to a new computer.

firewall

A software program or hardware device that protects networks from unauthorized data by blocking unsolicited traffic.

FireWire connection

A high-speed serial bus developed by Apple and Texas Instruments that allows for the connection of up to 63 devices. Originally a trademarked term for IEEE 1394, but is now used interchangeably.

firmware

Software stored in memory chips that retains data whether or not power to the computer is on.

first response

Refers to the individual and the immediate actions that follow an incident.

fixboot

A command line tool used to create a new partition boot sector to a hard drive partition.

fixmbr

A command line tool used to repair the master boot recovery record of the boot partition.

flash drive

See SSD.

Flash memory

A type of non-volatile storage method that provides devices with quick access to data.

flashing

Updating firmware electronically.

folder

See directory.

form factor

The size and shape of a given component. Often used in terms of motherboard and drive characteristics.

formed-character printer

Any type of impact printer that functions like a typewriter, by pressing preformed characters against the ink ribbon to deposit the ink on the page.

frontlight

A form of lighting devices from the front of the display.

full duplex

Permits simultaneous two-way communication.

fuser assembly

A component in a laser printer that uses two rollers to heat toner particles, melting them onto the paper.

gadget

A mini application in Windows that can perform an information display task.

gaming PC

A computer that is equipped with powerful graphics capabilities, fast processing capabilities, and a large amount of memory, to support the needs of gaming software applications.

GAN

(global area network) Any worldwide network.

gateway

A device, software, or system that converts data between incompatible systems.

generator

A power protection device that creates its own electricity through the use of motors.

geotracking

Uses the GPS mobile technology component to constantly track and update device's location with applications that share and use positioning information.

GPRS

(General Packet Radio Service) A standard for wireless communications that runs at speeds up to 115 kbps and that supports a wide range of bandwidths.

GPS

Technology that determines the location, weather, and time zone information of a device using the satellite navigation system.

GPU

(Graphics Processing Unit) An integrated circuit that is specially configured to accelerate the rendering of images that are intended for output to a display device.

gyroscope

Mobile technology that changes the orientation of the device by reading the x and y coordinates of device's position.

half duplex

Permits two-way communication, but only in one direction at a time.

hard drive sanitation

The method used to repeatedly delete and overwrite any traces or bits of sensitive data that may remain on a hard drive after data wiping has been done.

HDD

(hard disk drive) A personal computer storage device that uses fixed media and magnetic data storage.

HDMI

(High-Definition Multimedia Interface) The first industry-supported uncompressed, all-digital audio/video interface that uses a single cable to provide an interface between any audio/video source

and an audio and/or video monitor.

heat sink

A cooling device that is directly attached to the CPU to provide direct cooling using metal fins to increase its surface area to aid in heat dissipation.

heavy-duty MFD

A large network-enabled MFD capable of handling the documentation needs of an entire office.

hertz

A measure of the number of cycles per second in an analog signal. One cycle per second equals one hertz.

Hibernate

A power option available in Windows environments in which the computer will store whatever is currently in memory on the hard disk and shut down, and then return to the state it was in upon hibernation when it is awakened.

high-level formatting

See standard formatting.

hoax

Any message containing incorrect or misleading information that is disseminated to multiple users through unofficial channels.

HomeGroup

A utility unique to the Windows 7 Control Panel through which users can set up a home network and add users or computers to the group in order to share resources such as files and printers.

host

In a centralized network, the computer that controls network functions. In a TCP/IP network, any computer.

host machine

In virtualization technology, the computer on which the virtual environment is installed and which manages the VMs.

host or personal firewall

A firewall installed on a single or home computer.

hot swapping

Replacing a device without needing to power down the PC during removal of the old device or

installation of the new device. Also referred to as hot plug or hot insertion.

HTPC

(home theater PC) A computer system that is dedicated and configured to store and stream digital movies, either from a local hard drive or through an online subscription service.

hub

A device that connects multiple twisted pair segments together to form a single network segment.

HVD

(high-voltage differential) A SCSI signaling scheme that uses two wires, one for data and one for the inverse of data. HVD devices use high voltage and cannot be used on a single-ended SCSI chain.

hybrid topology

Any topology that exhibits the characteristics of more than one standard topology.

hypervisor

In virtualization technology, an application that is installed on the host machine and is used to configure and manage the VMs running on the host.

IEEE

(Institute of Electrical and Electronic Engineers) Pronounced "I-triple-E." An organization of scientists, engineers, and students of electronics and related fields whose technical and standards committees develop, publish, and revise computing and telecommunications standards.

IEEE 802.16

A series of wireless broadband standards wireless metropolitan area networks. See WiMAX.

imaging

The process of creating a computer image from one main computer, called the reference computer, and copying that image onto one or more other computers, called the target computers, as a method of installing an operating system and other programs.

IMAP4

(Internet Mail Access Protocol) A protocol used to retrieve email messages and folders from a mail server.

impact printer

Any type of printer that strikes a component directly against the paper or ink to create characters on the paper.

impersonation

An approach in which an attacker pretends to be someone they are not, typically an average user in distress, or a help-desk representative.

in-place upgrade

The process of installing a newer version of an operating system without first removing the existing operating system that is currently installed on the computer.

in-rush

A surge or spike that is caused when a device that uses a large amount of current is started.

incident report

A record of any instance where a person is injured or computer equipment is damaged due to environmental issues. Also, a record of accidents involving hazardous materials, such as chemical spills, that could have an impact on the environment itself.

inkjet printer

A printer that forms images by spraying ink on the paper.

input device

A personal computer component that enables users to enter data or instructions into a computer.

integrated circuit

An electronic component consisting of several transistors and resistors, connected together on a semiconductor chip.

integration components

Software available for Windows client virtualization solutions that enable you to share resources between the host operating system and the VM more efficiently.

interference

Within wireless networking, the phenomenon by which radio waves from other devices interfere with the 802.11 wireless signals.

Internet appliance

A device that allows quick easy access to the Internet.

inverter

A laptop component that converts DC power to AC power for the display.

iOS

The operating system designed for Apple devices. It is the base software that allows all other applications to run on an iPhone, iPod touch, or iPad.

IP

(Internet Protocol) A group of rules for sending data across a network. Communication on the Internet is based on the IP protocol.

IP version 6

An Internet standard that increases the available pool of IP addresses by implementing a 128-bit binary address space.

ipconfig

A command line tool used to verify the configuration of TCP/IP and to release or renew DHCP IP address leases.

IPv4 address

A 32-bit binary number assigned to a computer on a TCP/IP network.

IPv6 address

The unique 128 bit identification assigned to an interface on the IPv6 Internet.

IR

(infrared) A form of wireless transmission in which signals are sent via pulses of infrared light.

IR waves

(infrared waves) Electromagnetic waves with frequencies ranging from 300 GHz to 400 THz.

iSCSI

(Internet SCSI) A protocol that serializes SCSI commands so that they can be transferred over a TCP/IP network.

iSCSI Initiator

A Windows 7 Administrative Tool that enables you to configure advanced connections between network storage devices.

ISDN

A digital transmission technology that carries both voice and data over digital phone lines or PSTN wires.

ISP

(Internet Service Provider) A company that provides access to the Internet.

IV

(initialization vector) A technique used in cryptography to generate random numbers to be used along

with a secret key to provide data encryption.

IV attack

An attack where the attacker is able to predict or control the IV of an encryption process, thus giving the attacker access to view the encrypted data that is supposed to be hidden from everyone else except the user or network.

jumper

A set of pins and connectors used to configure hardware settings. You physically connect or disconnect a circuit by adding or removing a jumper to the block.

jumper block

A small rectangular connector, from a pair of pins attached to the system board or add-on card.

key fobs

Security devices small enough to attach to a key chain that contain identification information used to gain access to a physical entryway.

kill

A command line tool used to stop or terminate a process that is running.

KVM switch

(keyboard, video, mouse) A device that allows a computer user to control multiple computers with a single keyboard and mouse, with the display sent to a single monitor.

LAN

(local area network) A self-contained network that spans a small area, such as a single building, floor, or room.

laptop computer

A complete computer system that is small, lightweight, and portable.

laser printer

A type of printer that forms high-quality images on one page of paper at a time, by using a laser beam, toner, and an electrophotographic drum.

LC

(Local Connector) A small form factor ceramic ferrule connector for both single-mode and multimode fiber.

LCD

(Liquid Crystal Display) A type of flat-panel display that uses Cold Cathode Fluorescent Lamps as

the source of backlight and that comes in large-screen sizes of 17 inches and more, with high screen resolution and high color depth.

LDAP

(Lightweight Directory Access Protocol) A communications protocol that defines how a client can access information, perform operations, and share directory data on a directory server.

least privilege

The principle that establishes that users and software should only have the minimal level of access that is necessary for them to perform the duties required of them.

LED

(light emitting diode) An electrical component frequently used as an indicator light on network adapters and other types of network equipment.

LED display

A display device that uses either Dynamic RGB light emitting diodes or White Edge-light emitting diodes as the light source.

LED printer

A type of printer that uses LEDs to print.

line noise

A power problem that is caused by a fluctuation in electrical current.

link light

An indicator on a network adapter that lights up when a network signal is detected.

Linux

An open-standards UNIX derivative originally developed and released by a Finnish computer science student named Linus Torvalds.

Linux distribution

A complete Linux implementation, including kernel, shell, applications, and utilities, that is packaged, distributed, and supported by a software vendor.

liquid-based cooling

Cooling methods that circulate a liquid or liquefied gas, such as water or freon, past the CPU to keep it cool.

Local Area Connection

A Windows troubleshooting tool used to verify that the computer is connected to the network and able

to send and receive data.

local printer

A logical printer that is managed by the local computer, where the print device is generally directly attached.

Local Security Policy

An administrative tool that is used to view and edit the security settings for group policies.

local shares

Folders that are created on the local network by individual users and then shared with other network users via shared folder permissions.

Local Users and Groups

An administrative tool that is used to manage user accounts on the local system.

lockup error

An error condition that causes the system or an application to stop responding to user input.

logic bomb

A piece of code that sits dormant on a user's computer until it is triggered by a specific event, such as a specific date. Once the code is triggered, the logic bomb "detonates," erasing and corrupting data on the user's computer.

loopback plug

A special connector used for diagnosing network transmission problems that redirects electrical signals back to the transmitting system.

LOS

(Line-of-Sight) Wireless signals that travel over a direct visual path from a transmitter to a receiver.

low-level formatting

The process of writing track sector markings on a hard disk.

LTFS

(Linear Tape File Systems) An IBM specification that enables data stored on magnetic tapes to be accessed in a file format.

lumens

The unit of measurement for visible light that is being emitted from a light source.

LVD

(low-voltage differential) A SCSI signaling technique that uses two wires, one for data and one for the inverse of data. LVD devices use a low voltage and can be used on a single-ended SCSI chain.

MAC address

(Media Access Control address) Same as the physical address.

magnetic core memory

Memory that stores binary data (0 or 1) in the orientation of magnetic charges in ferrite cores about one-sixteenth-inch in diameter.

malicious software

Any unwanted software that has the potential to damage a system or create a nuisance condition.

malware

Any unwanted software that has the potential to damage a system, impede performance, or create a nuisance condition.

MAN

(metropolitan area network) A network that covers an area equivalent to a city or other municipality.

Mark I

A programmable, electromechanical calculator that combined 78 adding machines to perform three calculations per second. It was designed by Howard Aiken, built by IBM, and installed at Harvard in 1944.

MBR

(Master Boot Record) The first sector of a partitioned storage device, used for booting the computer and often a target of malware.

md

A command line tool used to create a directory.

media tester

See cable tester.

memory

A personal computer component that provides temporary workspace for the processor.

memory dump

The process of writing the contents of system memory at the time of a stop error to a file on the hard disk prior to system shutdown.

memory module

A system unit component that holds a group of memory chips that act as a single memory chip.

mesh topology

A network topology in which each node has a direct, point-to-point connection to every other node.

MFD

(multi-function device) A piece of office equipment that performs the functions of a number of other specialized devices.

microATX

Introduced in late 1997, and is often referred to as µATX, and has a maximum size of 9.6 inches by 9.6 inches.

MicroDIMM

(Micro Dual Inline Memory Module) A memory module standard used in small, sub-compact notebooks.

microprocessor

A complete central processing unit on a single chip, the microprocessor controls the operation of all the other computer components.

Mini-ATX

A smaller version of the full ATX board with a maximum size of 11.2 inches by 8.2 inches.

Mini-BNC

A bayonet-style connector using the traditional BNC connection method.

Mini-HDMI

(Mini High-Definition Multimedia Interface) A smaller version of the full size HDMI connector, except that it is specified for use with portable devices.

mini-ITX

A small compact board that fit the same form factor as the ATX, and the micro-ATX boards. They have a maximum size of 6.7 inches by 6.6 inches.

Mini-PCIe

(PCI Express Mini Card) An extremely small expansion card, often just a few centimeters in length used to increase communication abilities by providing network adapters or modems and supports various connections and buses.

mirroring

A disk fault-tolerance method in which data from an entire partition is copied onto a second drive.

modem

A device that modulates and demodulates data over an analog signal sent via a telephone line.

motherboard

The main circuit board in a computer that acts as the backbone for the entire computer system. Also referred to as the system board.

MSConfig

A system utility that is specifically used to troubleshoot any issues with the system startup process.

MSDS

(Material Safety Data Sheet) A technical bulletin designed to give users and emergency personnel information about the proper procedures of storage and handling of a hazardous substance.

MT-RJ

(Mechanical Transfer Registered Jack) Also called a Fiber Jack connector, is a compact snap-to-lock connector used with multimode fiber.

multi-factor authentication

Any authentication scheme that requires validation of at least two of the possible authentication factors.

multimedia device

A computer peripheral or internal component that transfers sound, images or both to or from a personal computer.

multimeter

An electronic instrument used to measure voltage, current, and resistance.

multitouch

The technology used on the surface of the touch screen on tablets and other mobile devices that can recognize more than one contact on the surface at once.

mutual authentication

A security mechanism that requires that each party in a communication verifies its identity.

Napier's Bones

A set of rectangular rods with numbers etched on them that let users do multiplication by adding the

numbers on properly positioned rods. Precursor to the slide rule.

NAS

(network-attached storage) A data storage device that can be connected to a network to provide direct data access and file sharing to multiple computing devices attached to the network.

NAT

(Network Address Translation) A simple form of Internet connection and security that conceals internal addressing schemes from the public Internet.

native resolution

The fixed resolution for LCD or other flat panel display devices.

nbtstat

A command line tool used to display TCP/IP information and other information for a remote computer.

net

A command line tool used to manage Microsoft network resources from a command line.

netstat

A command line tool used to show the status of each active network connection.

network

A group of connected computers that are connected together to communicate and share resources.

network directory

A centralized database that includes objects such as servers, clients, computers, user names, and passwords. Also called directory service.

Network Interference

The disruption of normal data transmissions over a network.

network share

See share.

network topology

A specification that determines the network's overall layout and transmission and flow patterns.

network-based firewall

A hardware/software combination that protects all the computers on a network behind the firewall.

network-based printer

A shared print device managed by a network print server. It's represented as a logical printer object on the client computer that accesses the server.

network-connected printer

Any print device than can connect directly to the network with a network adapter rather than using a physical cable to connect to a local computer or print server device.

NIC

(network interface card) An expansion card that enables a PC to connect to a LAN. Also referred to as a network adapter.

NLOS

(Non-Line-of-Sight) Wireless signals that reach a receiver through reflections and obstructions within the visual path in the environment.

node

A generalized term for any network device with its own address.

Northbridge

A component of the chipset that controls the system memory and the AGP video ports, and sometimes the cache memory.

nslookup

A command line tool used to verify that the computer can connect to a DNS server and successfully find an IP address for a given computer name.

Offline Files

A utility unique to the Windows Vista Control Panel that is used to enable or disable offline files and configure the settings for offline files.

OLED display

(organic light emitting diode) A type of LED flat panel display device that uses organic compounds that emit light when subjected to an electric current.

Open Handset Alliance

An association of 84 firms for developing open standards for mobile devices.

open source

Refers to application code, operating systems, and programming languages that are developed, published and shared among the developer and professional community.

optical disk

A personal computer storage device that stores data optically, rather than magnetically.

optical drive

A computer drive that is either internal or external to a computer system that reads and writes data to an optical disk.

organizational policy

A document that convey the corporate guidelines and philosophy to employees.

OS X

The proprietary operating system developed by Apple® Computing, Inc. and deployed on all Apple computers.

packet sniffing

An attack on wireless networks where an attacker captures data and registers data flows in order to analyze what data is contained in a packet.

page

A section of memory addresses in which a unit of data can be stored.

page fault

An interrupt generated when an application requests data that is no longer present in its virtual memory location.

pagefile

In a virtual-memory system, the section of the hard disk used to store memory contents that have been swapped out of physical RAM. In Windows systems, the pagefile is called Pagefile.sys.

paging

See swapping.

pairing

The process two devices use to establish a wireless connection through Bluetooth.

PAN

(personal area network) A network of devices used by a single individual.

parallel connection

A personal computer connection type that transfers data, usually 8 bits at a time, over eight wires, and is often used for a printer.

parity

An error correction method for electronic communications.

partitioning

The process of dividing a single hard disk into isolated sections that function as separate physical hard drives, called partitions.

Pascaline machine

A calculating machine that could add and subtract, developed in 1642 by Blaise Pascal.

PATA

(Parallel Advanced Technology Attachment) A type of hard drive that requires a parallel data channel to connect a disk controller to the disk drive. Also referred to as ATA, IDE, EIDE, or UDMA.

patch

Fixes or updates for a software program or application, designed to eliminate known bugs or vulnerabilities and improve performance.

patch management

The practice of monitoring for, evaluating, testing, and installing software patches and updates.

PC

(personal computer) Stand-alone, single-user, desktop-size or smaller computers that can function independently. PC used to refer to any personal computer, but now refers to personal computers that follow the original design by IBM, use Intel or compatible chips, and usually have some version of Windows as an operating system.

PC card

A credit-card-sized expansion card that is used in portable computers rather than the full-sized expansion cards used in desktop systems.

PCI

(Peripheral Component Interconnect) See PCI bus.

PCI bus

(Peripheral Component Interconnect bus) A peripheral bus commonly used in PCs that provides a high-speed data path between the CPU and peripheral devices.

PCI Express

(Peripheral Component Interconnect Express) A video adapter bus that is based on the PCI computer

bus. PCIe supports significantly enhanced performance over that of AGP.

PCIe

(Peripheral Component Interconnect Express) See PCI Express.

PCMCIA

(Personal Computer Memory Card International Association) See PC card.

PDA

(Personal Digital Assistants) Mobile devices used to manage personal information, such as address books, calendars, and emails.

peer-to-peer network

A network in which resource sharing, processing, and communications control are completely decentralized.

Pen and Input Devices

A utility unique to the Windows Vista Control Panel which is used to customize the settings for the pen and input devices that are used to interact with a tablet.

Performance Monitor

An administrative tool that monitors the state of services or daemons, processes, and resources on a system.

permissions

In Windows, security settings that control access to individual objects, such as files.

phishing

A type of email-based social engineering attack in which the attacker sends email from a spoofed source, such as a bank, to try to elicit private information from the victim.

physical address

For network adapter cards, a globally unique hexadecimal number burned into every adapter by the manufacturer.

physical security

The implementation and practice of various control mechanisms that are intended to restrict physical access to facilities.

piconet

A network of two to eight Bluetooth-enabled devices.

PictBridge

A technology that allows images to be printed directly on a printer from digital cameras.

ping

A command line tool used to test communications between two TCP/IP-based hosts.

pixel

The smallest discrete element on a display. A single pixel is composed of a red, a blue, and a green dot.

plasma

A type of flat panel that uses a gas mixture placed between two sheets of glass that have electrodes attached to their surfaces.

plasma display

A display device that uses xenon and neon rays and a flat panel of glass to provide a light source and images on screen.

plastics

The hard surfaces that protect the internal components of a laptop.

plenum

An air handling space, including ducts and other parts of the HVAC system in a building.

plenum cable

A grade of cable that does not give off noxious or poisonous gases when burned. Unlike PVC cable, plenum cable can be run through the plenum and firebreak walls.

PoE

(Power-over-Ethernet) An emerging technology standard that enables both power and data to be transmitted over an Ethernet cable.

pop-up

Windows or frames that load and appear automatically when a user connects to a particular web page.

pop-up blocker

Software that prevents windows or frames from automatically loading when users connect to websites that employ pop-ups.

POP3

(Post Office Protocol version 3) A protocol used to retrieve email from a mailbox on the mail server.

port

A hardware connection interface on a personal computer that enables devices to be connected to the computer, or the endpoint of a logical connection that client computers use to connect to specific server programs.

port replicator

A scaled-down version of a docking station with only the standard ports available.

POST

(Power-On Self Test) A built-in diagnostic program that is run every time a personal computer starts up.

POST card

A card can be plugged directly into the motherboard in an available expansion card slot that can read and display any error codes that get generated during the POST process of a computer.

power sag

See sag.

power supply

An internal computer component that converts line voltage AC power from an electrical outlet to the low-voltage DC power needed by system components.

power supply tester

A tool that connects to the power supply's 24-pin connector that tests the functionality of the unit.

Print Management

An administrative tool that is used to view and manage all of the printers and print servers installed on a network.

print queue

A list of jobs waiting to print.

print server

A computer somewhere on the network that manages a printer that has been shared for network clients to use.

printer

An output device that produces text and images from electronic content onto physical media such as paper or transparency film.

Printers

A utility in name only that is unique to the Windows Vista Control Panel, it is used to add, remove, and manage any printers installed on the computer. The Printers utility in Vista replaced the Printers and Faxes utility in Windows XP and was replaced with the Devices and Printers utility in Windows 7.

private IP address

Addresses used by organizations for nodes that require IP connectivity within their enterprise network, but do not require external connections to the global Internet.

Problem Reports and Solutions

A utility unique to the Windows Vista Control Panel that displays any recent problems that Windows has encountered and provides links to troubleshooting resources.

proxy

A system that acts as an intermediary for requests for resources.

PSTN

(Public Switched Telephone Network) An international telephone system that carries analog voice data.

public IP addresses

Addresses that can be used by organizations that can also be shared with external networks.

punch down tool

A tool used in a wiring closet to connect cable wires directly to a patch panel.

PVC

(polyvinyl chloride) A flexible rubber-like plastic used to surround some twisted pair cabling. It is flexible and inexpensive, but gives off noxious or poisonous gases when burned.

QoS

(Quality of Service) A set of parameters that controls the level of quality provided to different types of network traffic.

radio networking

A form of wireless communication in which signals are sent via RF waves, in the 10 KHz to 1 GHz range, to wireless antennas.

RAID

(Redundant Array of Independent or Inexpensive Disks) A set of vendor-independent specifications

for fault-tolerant configurations on multiple-disk systems.

RAM

(Random Access Memory) A computer storage method that functions as a computer's main memory.

RAM chip

An integrated circuit that acts as the computer's primary temporary storage place for data.

RAM module

See RAM chip.

RCA

(Radio Corporation of America) A cable and connector that is used to carry audio and video transmissions to and from a variety devices such as TVs, digital cameras, and gaming systems.

rd

A command line tool used to delete a directory.

ReadyBoost

A performance enhancer, available on Windows Vista and Windows 7, that allows the user to supplement the computer's memory with an external storage device like a flash drive.

Recovery Console

A minimal version of Windows XP Professional that provides a command-line interface (CLI) to a Windows XP Professional installation.

reference computer

The main computer in the imaging process.

refresh rate

The number of times per second that the monitor is “refreshed,” or scanned to illuminate the pixels.

Registry

The central configuration database where Windows stores and retrieves startup settings, hardware and software configuration information, and information for local user accounts.

regsvr32

A troubleshooting utility that registers and unregisters OLE controls such as DLL and ActiveX files.

Remote Desktop

A software application that operates a Windows computer from a remote location.

RemoteApp and Desktop Connections

A utility unique to the Windows 7 Control Panel in which users can access programs, remote computers, and virtual computers remotely that are made available by the network administrator.

resistor

An electronic component that resists the flow of electric current in an electronic circuit.

resolution

The number of pixels that make up the dimension of a display, represented in a ratio value as the number of horizontal pixels by vertical pixels.

RF

(radio frequency) A frequency in which network or other communications that take place using radio waves in the 10 KHz to 1 GHz range.

RFID badges

Security cards that contain a tag that reacts with the radio frequency of the identification system to allow or deny access.

RIMM

(Rambus Inline Memory Modules) A RAM form factor that has a metal cover that acts as a heat sink. Although they have the same number of pins, RIMMs have different pin settings and are not interchangeable with DIMMs and SDRAM

ring topology

A network topology in which all network nodes are connected in a circle.

riser card

A board that is plugged into the system board and provides additional slots for adapter cards.

robocopy

A command line tool used to copy files and folders/directories from one location to another, but with more options than the simple copy command.

rogue access point

An unauthorized wireless access point on a corporate or private network, which allows unauthorized individuals to connect to the network.

ROM

(Read-Only Memory) Memory that saves and stores a system data without a constant power source.

rootkit

Malicious code that is designed to hide the existence of processes or programs from normal detection methods and to gain continuous privileged access to a computer system.

rotation method

The schedule that determines how many backup tapes or other media sets are needed, and the sequence in which they are used and reused.

router

A networking device that connects multiple networks that use the same protocol.

RSA tokens

Small devices that include cryptographic keys, a digital signature, or even biometric information that is verified against an identification system to allow or deny access to a physical location, system, or network location.

S-Video

An analog video signal that carries the video data as two separate signals (brightness and color). S-Video works in 480i or 576i resolution.

sag

A momentary low-voltage power failure.

SAS

(Serial Attached SCSI) A serial version of the SCSI interface. SAS is a point-to-point architecture that uses a disk controller with four or more channels operating simultaneously. SAS also supports SATA drives, which can be mixed with SAS drives in a variety of configurations.

SATA

(Serial Advanced Technology Attachment) A type of hard drive that requires a serial data channel to connect the drive controller and the disk drives.

satellite

Provide extremely long-range wireless network transmissions to relay network signals from the network service provider to individual customers.

SC

(Subscriber Connector or Standard Connector) Box-shaped connectors that snap into a receptacle. SC connectors are often used in a duplex configuration where two fibers are terminated into two SC connectors that are molded together.

screen calibration

The method used to update the sensors on the device to respond quicker and more effectively to tapping, swiping, and pinching components on the screen.

SCSI

(Small Computer System Interface) An older personal computer connection standard that provides high-performance data transfer between the SCSI device and the other components of the computer. Pronounced “scuzzy.”

SCSI ID

Identifiers assigned to each SCSI device connected to the bus. The ID numbers range from 1 to 15.

sector

An individual storage area on a formatted disk.

security policy

A formalized statement that defines how security will be implemented within a particular organization.

serial connection

A personal computer connection that transfers data one bit at a time over a single wire and is often used for an external modem.

server

A computer that provides services and resources on the network.

server-side virtualization

Takes place centrally on a server and utilizes one logical device, typically the server, to act as the host machine for the “guest” machines that virtually use the applications and programs provided by the host.

Service Packs

Comprehensive software updates that generally include all prior patches and updates, but which can also include important new features and functions.

Services

An administrative tool that is used to view all of the services that run in the background on the system.

sfc

(System File Checker) A command line tool used to verify system files and replace them, if needed.

SFTP

(Secure FTP) A secure replacement for FTP that uses the SSH protocol to provide secure data

connections.

Shadow Copy

A feature available on Windows XP and newer operating systems that creates backup copies or snapshots of the system's data and stores them locally or to an external location, either manually or at regularly scheduled intervals.

share

A network resource, such as a disk, folder, or printer, that is available to other computer users on the network.

shoulder surfing

A human-based attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN.

shutdown

A command line tool used to log off, restart, or shut down the system.

Sidebar

A designated area of the Windows 7 and Windows Vista desktop, displayed vertically along the side of the desktop, where users can add gadgets of their choice to provide information and access to frequently used tools or programs.

signature

A code pattern that identifies a virus. Also called a definition.

SIMM

(Single In-line Memory Modules) A RAM form factor with a 32-bit data path.

SLA

(Service Level Agreement) An agreement entered into by the transmitter, ISP and the receiver, subscriber.

Sleep

A power option available in Windows Vista, Windows 7, Windows Server 2008, and Apple OSs, in which the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM.

SMA

(Sub Multi Assembly or Sub Miniature type A) Connectors that use a threaded ferrule on the outside to lock the connector in place.

smart card

A device similar to a credit card that can store authentication information, such as a user's private key, on an embedded microchip.

smartphones

High-end mobile devices that provide users with a wide range of functions such as, portable media players, video cameras, GPS, high-resolution touch screens, high-speed Wi-Fi, web browsers, and mobile broadband.

SMB

(Server Message Block) A protocol that works on the Application layer and is used to share files, serial ports, printers, and communications devices, including mail slots and named pipes, between computers.

SNMP

(Simple Network Management Protocol) An Application-layer protocol used to exchange information between network devices.

social engineering attack

A type of attack where the goal is to obtain sensitive data, including user names and passwords, from network users through deception and trickery.

SODIMM

(Small Outline Dual In-line Memory Module) Memory that is half the size of DIMMs, are available in 32- or 64-bit data paths, and are commonly found in laptops and iMac systems.

software diagnostic tool

A computer repair tool that contains programs that test hardware and software components. Also referred to as utility.

SOHO MFD

(small office/home office multi-function device) A medium-sized network-enabled MFD suitable for small and home offices with enhanced printing, scanning, copying, and faxing functions.

SOHO network

(small office/home office) A small network that provides connectivity and resource sharing for a small office or home office.

soldered

A means of securing electronic components to a circuit board by using a combination of lead, tin, and silver (solder) and a tool called a soldering iron.

solid ink printer

A type of printer that uses ink from melted solid-ink sticks.

Southbridge

A component of the chipset that controls input/output functions, the system clock, drives and buses, APM power management, and various other devices.

spam

Originally, frequent and repetitive postings in electronic bulletin boards; more commonly, unsolicited or distasteful commercial email from anonymous sources.

spam blocker

Software that detects specific words or phrases that are known to be included in spam messages and rejects the messages as unwanted.

speed light

An indicator on a network adapter that shows whether the adapter is operating at 10 Mbps, 100 Mbps, or 1,000 Mbps.

spike

A short-term, high-voltage power malfunction.

spim

An IM-based attack similar to spam that is propagated through instant messaging instead of through email.

spoofing

A human-based or software-based attack where the goal is to pretend to be someone else for the purpose of identity concealment. Spoofing can occur in IP addresses, MAC addresses, and email.

spyware

Unwanted software that collects personal user data from a system and transmits it to a third party.

SSA

(Serial Storage Architecture) A fault-tolerant peripheral interface that transfers data at 80 and 160 MBps. SSA uses SCSI commands, allowing existing software to drive SSA peripherals such as disk drives. SSA uses a ring architecture that supports up to 128 devices; if one fails, the remaining devices continue to run. SSA distances are 25 meters over copper and 2.4 kilometers over fiber. SSA was designed to provide an alternative to Fibre Channel, but has not been as widely used.

SSD

(solid state drive) A personal computer storage device that stores data in non-volatile special memory instead of on disks or tape.

SSH

(Secure Shell) A protocol that enables a user or application to log on to another computer over a network, execute commands, and manage files.

SSID

(Service Set Identifier) A 32-bit alphanumeric string that identifies a wireless access point and all devices that connect to it.

SSL

(Secure Sockets Layer) A security protocol that uses certificates for authentication and encryption to protect web communication.

ST

(Straight Tip) Connects multimode fiber, ST connectors look like BNC connectors.

standard formatting

An operating system function that builds file systems on drives and partitions.

Standby

A power option available in Windows 98, Windows Server 2003, and Windows XP, in which the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM.

star topology

A network topology that uses a central connectivity device with separate point-to-point connections to each node.

static addressing

Configuring TCP/IP statically on a network and requires that an administrator visit each node to manually enter IP address information for that node.

static electricity

The buildup up of stationary electrical charge on any object.

Stepped Reckoner

A mechanical calculator developed by Gottfried von Leibniz that improved Pascal's design to include multiplication and division.

stop error

A system error severe enough to stop all processes and shut the system down without warning. Often referred to as "blue-screen errors" in Windows because they generate an error message screen with a blue background.

storage device

A computer component that enables users to save data for reuse at a later time, even after the personal computer is shut down and restarted.

striping

A disk-performance-enhancement feature in which data is spread across multiple drives to improve read and write access speeds.

strong password

A password that meets the complexity requirements that are set by a system administrator and documented in a password policy.

stuck pixels

Pixels that only show one color of light, so they appear out of place when the display is on.

subnet mask

A 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions.

surge suppressor

A power protection device that provides power protection circuits that can reduce or eliminate the impact of surges and spikes.

Suspend

A power option available in Windows 95 and Linux, in which the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM.

swapping

In a virtual memory system, the process of moving data back and forth from physical RAM to the pagefile. Also called paging.

switch

A "smart" network hardware device that joins multiple network segments together.

system BIOS

The BIOS that sets the computer’s configuration and environment when the system is powered on.

system board

The same as motherboard.

system bus

The primary communication pathway between a CPU and other parts of the chipset. The system bus enables data transfer between the CPU, BIOS, memory, and the other buses in the computer. Also referred to as frontside bus or local bus.

System Configuration

An administrative tool that is used to identify and manage issues that may be causing the system to run improperly at startup.

system files

The files necessary for the operating system to function properly.

System Restore

A utility available in Windows XP, Windows Vista, and Windows 7 that monitors the system for changes to core system files, drivers, and the Registry, and creates restore points to be used to help restore the system if a failure occurs.

system restore point

A snapshot of the system configuration at a given moment in time that contains information about any changes to these components and is stored on the computer's hard disk. Restore points can be used to restore system settings to an earlier state without affecting changes in user data since that time.

system unit

A personal computer component that includes other devices necessary for the computer to function, including the chassis, power supply, cooling system, system board, microprocessor, memory chips, disk drives, adapter cards, and ports for connecting external devices. Often referred to as a box, main unit, or base unit.

Tablet PC Settings

A utility unique to the Windows Vista Control Panel where the user can configure settings for a tablet PC running Windows Vista.

tablets

Mobile computers that function similarly to a full sized desktop computer come with an integrated touchscreen and virtual onscreen keyboard.

tape drive

A personal computer storage device that stores data magnetically on a removable tape.

target computer

The computer that has the image installed on it in the imaging process.

Task Manager

A basic system-diagnostic and performance-monitoring tool included with the Windows operating system.

Task Scheduler

An administrative tool that allows the user to create and manage certain system tasks that will be automatically carried out by the computer at predetermined times.

TCP

(Transmission Control Protocol) A connection-oriented, guaranteed-delivery protocol used to send data packets between computers over a network such as the Internet.

TCP/IP

(Transmission Control Protocol/Internet Protocol) A nonproprietary, routable network protocol suite that enables computers to communicate over a network, including the Internet.

terminal

A client node on a centralized network, with few or no local computing resources of its own.

termination

Adding a resistor to the end of a coax network segment to prevent reflections that would interfere with the proper reception of network signals.

thermal dye transfer printer

A sophisticated type of color printer that uses heat to diffuse dye from color ribbons onto special paper or transparency blanks to produce continuous-tone output similar in quality to a photographic print. Also called dye sublimation printer.

thermal paper

Paper that contains a chemical designed to react with the heating element of a thermal printer to create images on paper.

thermal paste

A paste that is used to connect a heat sink to a CPU to provide a liquid thermally conductive compound gel that fills any gaps between the CPU and the heat sink to permit a more efficient transference of heat from the processor to the heat sink.

thermal printer

Any printer that uses heat to create the image on the paper with dye or ink from ribbons or with heated pins.

thermal wax transfer printer

A printer that uses a thermal printhead to melt wax-based ink from a transfer ribbon onto the paper.

thick client

A computer that performs most or all of the processing it requires to complete a given task.

thin client

A computer that depends on another computer such as a server to run most of its programs, processes, and services.

TIA

(Telecommunication Industry Association) A standards and trades organization that develops industry standards for technologies such as network cabling.

TKIP

(Temporal Key Integrity Protocol) A security protocol created by the IEEE 802.11i task group to replace WEP.

tlist

A command line tool used to display all the processes currently running on the system.

TLS

(Transport Layer Security) A security protocol that protects sensitive communication from eavesdropping and tampering by using a secure, encrypted, and authenticated channel over a TCP/IP connection.

token

A physical or virtual object that stores authentication information.

toner

An electrostatic-sensitive dry ink substance used in laser printers.

tracert

A command line tool used to determine the route that the computer uses to send a packet to its destination. If tracert is unsuccessful, you can use the results generated to determine at what point communications are failing.

traces

Wires etched on to the motherboard to provide electrical pathways.

trackpoint

A small button found on some laptops that enables you to move the mouse pointer when no mouse is connected to the computer.

transistor

A device containing semiconductor material that can amplify a signal or open and close a circuit. In computers, transistors function as electronic switches.

transistors

Switches that are etched on one sliver of a semiconductor that can be opened or closed when conducting electricity.

triboelectric generation

Using friction to create a static charge.

Trojan horse

Malicious code that masquerades as a harmless file. When a user executes it, thinking it is a harmless application, it destroys and corrupts data on the user's hard drive.

Troubleshooting

A utility unique to the Windows 7 Control Panel that provides troubleshooting resources for common Windows problems.

tunneling

A data transport technique in which a data packet is transferred inside the frame or packet of another protocol, enabling the infrastructure of one network to be used to travel to another network.

twisted pair

A type of cable in which multiple insulated conductors are twisted together and clad in a protective and insulating outer jacket.

UAC

(User Account Control) An enhanced security feature of Vista and Windows 7 that aims to limit the privileges of a standard user unless a computer administrator decides otherwise.

UDP

(User Datagram Protocol) A connectionless, best-effort delivery protocol used to send data packets between computers over a network such as the Internet.

UNIVAC

The Universal Automatic Computer, completed in 1951 by Eckert and Mauchly for the U.S. Bureau of

the Census. It was the first commercial computer in the United States and could handle both numerical and alphabetical information.

UNIX

A family of operating systems originally developed at Bell Laboratories and characterized by portability, multiuser support, and built-in multitasking and networking functions.

UPS

(uninterruptible power supply) A device that continues to provide power to connected circuits when the main source of power becomes unavailable. This can help save computer components from damage due to power problems such as power failures, spikes, and sags.

USB

(universal serial bus) A hardware interface standard designed to provide connections for numerous peripherals.

USB connection

A personal computer connection that enables you to connect multiple peripherals to a single port with high performance and minimal device configuration.

user account

A collection of credentials and important information about a person with access to the system, including the rights and privileges assigned to the user.

user authentication

A network security measure in which a computer user or some other network component proves its identity in order to gain access to network resources.

USMT

(User State Migration Tool) A command-line utility that copies files and settings from one Microsoft Windows computer to another.

vacuum tube

A sealed glass or metal container that controls a flow of electrons through a vacuum.

VDI

(Virtual Desktop Infrastructure) A computing environment where the personal computing component is separated from a physical machine using desktop virtualization.

VGA

(Video Graphics Array) A connector used for monitors.

virtual desktops

The virtual machines that run on a desktop operating system.

virtual memory

The allocation by the computer system of a portion of the hard disk as if it was physical RAM.

virtualization

The technological process of creating a virtual version of a computer environment by separating the elements of the computing environment from each other and from the physical hardware it runs on via an additional software layer.

virus

A piece of code that spreads from one computer to another by attaching itself to other files.

vishing

A human-based attack where the goal is to extract personal, financial, or confidential information from the victim by using services such as the telephone system and IP-based voice messaging services, VoIP, as the communication medium.

VM

(virtual machine) In virtualization, a software implementation or emulation of a host machine, which is created by the hypervisor and run independently from the host on which they are installed.

VMM

(Virtual Memory Manager) The Windows system component responsible for managing physical-to-virtual memory mappings and virtual memory assignments.

VoIP

(Voice over IP) A Voice over Data implementation in which voice signals are transmitted over IP networks.

volume

A single storage unit made up of free space that is located on a single file system, but which may reside on one or more disks or partitions.

VPN

(virtual private network) A private network that protects communications sent through a public network such as the Internet.

VPN protocol

A protocol that provides VPN functionality.

WAN

(wide area network) A network that spans multiple geographic locations, connecting multiple LANs using long-range transmission media.

WAP

(Wireless Access Point) A device that provides connection between wireless devices and can connect to wired networks.

war chalking

Using symbols to mark a sidewalk or wall to indicate that there is an open wireless network which may be offering Internet access.

war driving

The act of searching for instances of wireless LAN networks while in motion, using wireless tracking devices like PDAs, mobile phones, or laptops.

waveform

The shape of an analog signal when plotted on an oscilloscope or graph.

WEP

(Wired Equivalent Privacy) Provides 64-bit, 128-bit, and 256-bit encryption for wireless communication that uses the 802.11a and 802.11b protocols.

whaling

A form of phishing that targets individuals who are known or are believed to be wealthy.

Wi-Fi

The popular implementation of the 802.11b wireless standard.

WiMAX

(Worldwide Interoperability for Microwave Access) A packet-based wireless technology that provides wireless broadband access over long distances.

Windows Firewall with Advanced Security

An administrative tool that is used to manage advanced firewall settings for the computer and any remote computers connected to the network.

Windows Memory Diagnostic

An administrative tool that is used to check the RAM on the system and make sure that it is functioning appropriately and efficiently.

Windows security policies

Configuration settings within Windows operating systems that control the overall security behavior of the system.

WinPE

(Windows pre-installation environment) A lightweight version of Windows or Windows Server that can be used for deployment of the full version of the OS or for troubleshooting OS problems.

WinRE

(Windows Recovery Environment) A set of tools included in Windows Vista and Windows 7 that is used to help diagnose and repair errors on startup.

wire crimper

A tool that attaches media connectors to the ends of cables.

wire stripper

A tool that is often incorporated into a wire crimper and that enables the user to remove the protective coating from electrical wires.

wireless connection

A network connection that transmits signals without using physical network media.

wireless encryption

The process of concealing and protecting data during wireless transmissions.

Wireless Network Connection

A Windows troubleshooting tool used to verify that a computer or other wireless device is connected to the network and able to send and receive data.

wireless security

Any method of securing your wireless LAN network to prevent unauthorized network access and network data theft while ensuring that authorized users can connect to the network.

WOL

(Wake-on-LAN) A networking capability that is built into a device's NIC circuitry that allows a device to turn on, or power up when a network message is received by another computing device.

workgroup

A peer-to-peer Microsoft network model that groups computers together for organizational purposes, often deployed in homes and small offices.

worm

A piece of code that spreads from one computer to another on its own, not by attaching itself to another file.

WPA

(Wi-Fi Protected Access) A strong authentication security protocol that was introduced to address some of the shortcomings in the WEP protocol during the pending development of the 802.11i IEEE standard.

WPAN

(Wireless Personal Area Network) A network that connects devices in very close proximity but not through a wireless access point.

WWAN

(Wireless Wide Area Network) A computer network that enables users to wirelessly connect to their offices or the Internet via a cellular network. Sometimes referred to as wireless broadband.

xcopy

A command line tool used to copy files or directories from one location to another.

XP mode

A downloadable add-on for Windows 7 that allows users running Windows 7 to access and use Windows XP-compatible software and programs directly on their desktops.